

CERTIFICATION

# Study Guide

For the CAMS Examination



CERTIFICATION

# Study Guide

For the CAMS Examination



# STUDY GUIDE

## CAMS CERTIFICATION EXAM

SIXTH EDITION

*Task Force Executive Chair*

John J. Byrne, CAMS

*Project Manager*

Catalina Martinez

We would like to thank the following individuals for their significant contribution in the development of the CAMS Examination and Study Guide through the work of the CAMS Examination Task Force.

Bob Pasley, CAMS—*Task Force Chair*  
Kevin Anderson, CAMS—*Task Force Chair*  
Brian Stoeckert, CAMS—*Task Force Chair*  
Paul Osborne, CAMS—*Task Force Chair*  
Peter Wild, CAMS-Audit—*Task Force Vice Chair*  
Barbara Keller, CAMS—*Task Force Vice Chair*  
Hue Dang, CAMS-Audit (*ACAMS Asia*)  
Samantha Sheen, CAMS (*ACAMS Europe*)  
Rick Small, CAMS—*ACAMS Advisory Board*  
Nancy Saur, CAMS—*ACAMS Advisory Board*  
David Clark, CAMS—*ACAMS Advisory Board*  
Vasilios Chrisos, CAMS—*ACAMS Advisory Board*  
Anna Rentschler, CAMS—*ACAMS Advisory Board*  
Dennis Lormel, CAMS—*ACAMS Advisory Board*

Abbas Bou Diab, CAMS  
Angel Nguyen, CAMS  
Brian Vitale, CAMS-Audit  
Brigitte K. Miller, CAMS  
Christopher Bagnall, CAMS  
Christopher Randle, CAMS-Audit, CAMS-FCI  
Dave Dekkers, CAMS-Audit  
Deborah Hitzeroth, CAMS-FCI  
Donna Davidek, CAMS-Audit  
Ed Beemer, CAMS-FCI  
Eric Wathen, CAMS  
Gary Bagliebter, CAMS  
Iris Smith, CAMS-Audit  
Iwona Skornicka Castro, CAMS  
Jack Sonnenschein, CAMS-Audit  
Jeremy Brierley, CAMS  
Jim Vilker, CAMS  
Joel Conaty  
Jurgen Egberink, CAMS

Kenneth Simmons, CAMS-Audit  
Kok Cheong Leong, CAMS-Audit  
Lauren Kohr, CAMS-Audit  
Lindsay Dastrup, CAMS-Audit  
Margaret Silvers, CAMS  
Martin Dilly, CAMS-Audit  
Nancy Lake, CAMS-Audit, CAMS-FCI  
Peter Warrack, CAMS  
Rachele Byrne, CAMS  
Sean McCrossan, CAMS-FCI  
Sharon McCullough, CAMS  
Steve Gurdak, CAMS  
Susan Cannon, CAMS-Audit  
Susanne Wai Yin Ong, CAMS  
Tatiana Turculet, CAMS  
Venus Edano, CAMS  
William Aubrey Chapman, CAMS-Audit  
Yevgeniya Balyasna-Hooghiemstra, CAMS  
Zachary Miller, CAMS-FCI

ACAMS would also like to thank the ACAMS Chapters worldwide for their contribution in the development of the CAMS Examination.

*Special Contributor:* Gina Storelli, CAMS-Audit

# Table of Contents

## Introduction

About ACAMS .....	x
– ABOUT THE CAMS DESIGNATION .....	x

## Chapter 1

<b>Risks and Methods of Money Laundering and Terrorist Financing .....</b>	<b>1</b>
• <b>What Is Money Laundering? .....</b>	<b>1</b>
• <b>Three Stages in the Money Laundering Cycle .....</b>	<b>2</b>
The Economic and Social Consequences of Money Laundering .....	4
AML/CFT Compliance Programs and Individual Accountability .....	9
Methods of Money Laundering .....	10
Banks and Other Depository Institutions .....	11
– ELECTRONIC TRANSFERS OF FUNDS .....	11
– REMOTE DEPOSIT CAPTURE .....	12
– CORRESPONDENT BANKING .....	13
– PAYABLE-THROUGH ACCOUNTS .....	15
– CONCENTRATION ACCOUNTS .....	16
– PRIVATE BANKING .....	17
– USE OF PRIVATE INVESTMENT COMPANIES IN PRIVATE BANKING .....	18
– POLITICALLY EXPOSED PERSONS (PEPS) .....	19
– STRUCTURING .....	20
– MICROSTRUCTURING .....	22

Credit Unions and Building Societies .....	23
Nonbank Financial Institutions. ....	24
– CREDIT CARD INDUSTRY .....	24
– THIRD-PARTY PAYMENT PROCESSORS .....	25
– MONEY SERVICES BUSINESSES .....	26
– INSURANCE COMPANIES .....	30
– SECURITIES BROKER-DEALERS.....	32
• Variety and Complexity of Securities .....	33
• High-Risk Securities .....	33
• Multiple Layers and Third-Party Risk.....	34
Nonfinancial Businesses and Professions .....	36
– CASINOS .....	36
– DEALERS IN HIGH-VALUE ITEMS (PRECIOUS METALS, JEWELRY, ART, ETC.) .....	41
– TRAVEL AGENCIES.....	43
– VEHICLE SELLERS .....	44
– GATEKEEPERS: NOTARIES, ACCOUNTANTS, AUDITORS AND LAWYERS .....	45
– INVESTMENT AND COMMODITY ADVISORS.....	49
– TRUST AND COMPANY SERVICE PROVIDERS.....	50
– REAL ESTATE.....	52
International Trade Activity .....	55
– FREE TRADE ZONES.....	55
– TRADE-BASED MONEY LAUNDERING TECHNIQUES .....	55
– BLACK MARKET PESO EXCHANGE .....	58
• <b>Risk Associated With New Payment Products and Services .....</b>	<b>60</b>
Prepaid Cards, Mobile Payments and Internet-Based Payment Services.....	61
Virtual Currency .....	65

• <b>Corporate Vehicles Used to Facilitate Illicit Finance</b> .....	<b>67</b>
Public Companies and Private Limited Companies.....	<b>67</b>
– BEARER SHARES IN CORPORATE FORMATION.....	<b>68</b>
Shell and Shelf Companies .....	<b>69</b>
Trusts.....	<b>71</b>
Terrorist Financing.....	<b>72</b>
– DIFFERENCES AND SIMILARITIES BETWEEN TERRORIST FINANCING AND MONEY LAUNDERING .....	<b>73</b>
– DETECTING TERRORIST FINANCING .....	<b>74</b>
– HOW TERRORISTS RAISE, MOVE AND STORE FUNDS.....	<b>76</b>
Use of Hawala and Other Informal Value Transfer Systems.....	<b>76</b>
Use of Charities or Nonprofit Organizations (NPOs) .....	<b>79</b>
Emerging Risks for Terrorist Financing .....	<b>81</b>

## Chapter 2

<b>International AML/CFT Standards</b> .....	<b>87</b>
<b>Financial Action Task Force (FATF)</b> .....	<b>87</b>
FATF Objectives.....	<b>87</b>
FATF 40 Recommendations.....	<b>90</b>
FATF Members and Observers.....	<b>96</b>
Noncooperative Countries .....	<b>99</b>
The Basel Committee on Banking Supervision .....	<b>101</b>
History of the Basel Committee.....	<b>103</b>
European Union Directives on Money Laundering .....	<b>109</b>
– FIRST DIRECTIVE .....	<b>109</b>
– SECOND DIRECTIVE .....	<b>110</b>
– THIRD DIRECTIVE .....	<b>111</b>
– FOURTH DIRECTIVE .....	<b>112</b>
– OTHER RELEVANT LEGAL DOCUMENTS.....	<b>114</b>

<b>FATF-Style Regional Bodies.....</b>	<b>114</b>
– FATF-STYLE REGIONAL BODIES AND FATF ASSOCIATE MEMBERS.....	<b>114</b>
– ASIA/PACIFIC GROUP ON MONEY LAUNDERING (APG).....	<b>115</b>
– CARIBBEAN FINANCIAL ACTION TASK FORCE (CFATF).....	<b>116</b>
– COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES (MONEYVAL).....	<b>117</b>
– FINANCIAL ACTION TASK FORCE OF LATIN AMERICA (GAFILAT).....	<b>118</b>
– INTERGOVERNMENTAL ACTION GROUP AGAINST MONEY LAUNDERING IN WEST AFRICA (GIABA) .....	<b>118</b>
– MIDDLE EAST AND NORTH AFRICA FINANCIAL ACTION TASK FORCE (MENAFATF) .....	<b>119</b>
– EURASIAN GROUP ON COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM (EAG) .....	<b>119</b>
– EASTERN AND SOUTH AFRICAN ANTI-MONEY LAUNDERING GROUP (ESAAMLG) ....	<b>120</b>
– TASK FORCE ON MONEY LANDERING IN CENTRAL AFRICA (GABAC).....	<b>121</b>
<b>Organization of American States:</b>	
<b>Inter-American Drug Abuse Control Commission</b>	
<b>(Comisión Interamericana Para El Control Del Abuso De Drogas) .....</b>	<b>121</b>
<b>Egmont Group of Financial Intelligence Units.....</b>	<b>122</b>
<b>The Wolfsberg Group.....</b>	<b>124</b>
<b>The World Bank and the International Monetary Fund .....</b>	<b>128</b>
<b>Key U.S. Legislative and Regulatory Initiatives</b>	
<b>Applied to Transactions Internationally.....</b>	<b>131</b>
<b>USA PATRIOT Act .....</b>	<b>131</b>
<b>The Reach of the U.S. Criminal Money</b>	
<b>Laundering and Civil Forfeiture Laws .....</b>	<b>136</b>
<b>Office of Foreign Assets Control.....</b>	<b>137</b>

## Chapter 3

<b>Anti-Money Laundering/Counter-Terrorist Financing Compliance Programs .....</b>	<b>141</b>
• <b>Assessing AML/CFT Risk.....</b>	<b>142</b>
Introduction.....	142
Maintaining an AML/CFT Risk Model .....	143
Understanding AML/CFT Risk .....	144
AML/CFT Risk Scoring .....	145
Assessing The Dynamic Risk of Customers.....	146
AML/CFT Risk Identification .....	146
– CUSTOMER TYPE.....	147
– GEOGRAPHIC LOCATION.....	148
– PRODUCTS/SERVICES.....	149
• <b>AML/CFT Program .....</b>	<b>151</b>
The Elements of an AML/CFT Program.....	151
A System of Internal Policies, Procedures and Controls.....	151
– AML POLICIES, PROCEDURES AND CONTROLS.....	153
The Compliance Function.....	155
The Designation and Responsibilities of a Compliance Officer.....	155
– COMMUNICATION .....	155
– DELEGATION OF AML DUTIES .....	156
– COMPLIANCE OFFICER ACCOUNTABILITY.....	157
AML/CFT Training.....	158
– COMPONENTS OF AN EFFECTIVE TRAINING PROGRAM .....	158
– WHO TO TRAIN.....	158
– WHAT TO TRAIN ON.....	159
– HOW TO TRAIN.....	161
– WHEN TO TRAIN.....	162
– WHERE TO TRAIN .....	162

<b>Independent Audit</b> .....	<b>162</b>
– EVALUATING AN AML/CFT PROGRAM .....	<b>162</b>
<b>Establishing a Culture of Compliance</b> .....	<b>165</b>
<b>Know Your Customer</b> .....	<b>168</b>
– CUSTOMER DUE DILIGENCE .....	<b>168</b>
– MAIN ELEMENTS OF A CUSTOMER DUE DILIGENCE PROGRAM .....	<b>169</b>
– ENHANCED DUE DILIGENCE .....	<b>170</b>
– ENHANCED DUE DILIGENCE FOR HIGHER-RISK CUSTOMERS .....	<b>171</b>
– ACCOUNT OPENING, CUSTOMER IDENTIFICATION AND VERIFICATION .....	<b>171</b>
– CONSOLIDATED CUSTOMER DUE DILIGENCE .....	<b>176</b>
<b>Economic Sanctions</b> .....	<b>177</b>
– UNITED NATIONS .....	<b>177</b>
– EUROPEAN UNION .....	<b>177</b>
– UNITED STATES .....	<b>178</b>
<b>Sanctions List Screening</b> .....	<b>178</b>
<b>Politically Exposed Persons Screening</b> .....	<b>179</b>
<b>Know Your Employee</b> .....	<b>180</b>
<b>Suspicious or Unusual Transaction Monitoring and Reporting</b> .....	<b>182</b>
<b>Automated AML/CFT Solutions</b> .....	<b>183</b>
<b>Money Laundering and Terrorist Financing Red Flags</b> .....	<b>186</b>
– UNUSUAL CUSTOMER BEHAVIOR .....	<b>186</b>
– UNUSUAL CUSTOMER IDENTIFICATION CIRCUMSTANCES .....	<b>187</b>
– UNUSUAL CASH TRANSACTIONS .....	<b>187</b>
– UNUSUAL NONCASH DEPOSITS .....	<b>188</b>
– UNUSUAL WIRE TRANSFER TRANSACTIONS .....	<b>189</b>
– UNUSUAL SAFE DEPOSIT BOX ACTIVITY .....	<b>189</b>
– UNUSUAL ACTIVITY IN CREDIT TRANSACTIONS .....	<b>189</b>
– UNUSUAL COMMERCIAL ACCOUNT ACTIVITY .....	<b>190</b>
– UNUSUAL TRADE FINANCING TRANSACTIONS .....	<b>190</b>

– UNUSUAL INVESTMENT ACTIVITY.....	191
– OTHER UNUSUAL CUSTOMER ACTIVITY.....	191
– UNUSUAL EMPLOYEE ACTIVITY.....	191
– UNUSUAL ACTIVITY IN A MONEY REMITTER/ CURRENCY EXCHANGE HOUSE SETTING.....	192
– UNUSUAL ACTIVITY FOR VIRTUAL CURRENCY.....	192
– UNUSUAL ACTIVITY IN AN INSURANCE COMPANY SETTING.....	192
– UNUSUAL ACTIVITY IN A BROKER-DEALER SETTING.....	193
– UNUSUAL REAL ESTATE ACTIVITY.....	194
– UNUSUAL ACTIVITY FOR DEALERS OF PRECIOUS METALS AND HIGH-VALUE ITEMS.....	195
– UNUSUAL ACTIVITY INDICATIVE OF TRADE-BASED MONEY LAUNDERING.....	195
– UNUSUAL ACTIVITY INDICATIVE OF HUMAN SMUGGLING.....	196
– UNUSUAL ACTIVITY INDICATIVE OF HUMAN TRAFFICKING.....	197
– UNUSUAL ACTIVITY INDICATIVE OF POTENTIAL TERRORIST FINANCING.....	199

## Chapter 4

<b>Conducting and Responding to Investigations.....</b>	<b>203</b>
• <b>Investigations Initiated by the Financial Institution.....</b>	<b>203</b>
<b>Sources of Investigations.....</b>	<b>203</b>
– REGULATORY RECOMMENDATIONS OR OFFICIAL FINDINGS.....	203
– TRANSACTION MONITORING.....	204
– REFERRALS FROM CUSTOMER-FACING EMPLOYEES.....	204
– INTERNAL HOTLINES.....	205
– NEGATIVE MEDIA INFORMATION.....	205
– RECEIPT OF A GOVERNMENTAL SUBPOENA OR SEARCH WARRANT.....	205
SUBPOENA.....	206
SEARCH WARRANT.....	206
– ORDERS TO RESTRAIN OR FREEZE ACCOUNTS OR ASSETS.....	207

Conducting the Investigation.....	208
– UTILIZING THE INTERNET WHEN CONDUCTING FINANCIAL INVESTIGATIONS.....	209
STR Decision-Making Process.....	212
– FILING AN STR.....	213
– QUALITY ASSURANCE.....	213
– STR FILING OVERSIGHT/ESCALATION.....	213
Closing the Account.....	214
Communicating With Law Enforcement on STRs.....	215
Investigations Initiated by Law Enforcement.....	215
Decision to Prosecute a Financial Institution for Money Laundering Violations.....	216
Responding to a Law Enforcement Investigation Against a Financial Institution.....	217
Monitoring a Law Enforcement Investigation Against a Financial Institution.....	217
Cooperating With Law Enforcement During an Investigation Against a Financial Institution.....	218
Obtaining Counsel for an Investigation Against a Financial Institution.....	219
– RETAINING COUNSEL.....	219
– ATTORNEY-CLIENT PRIVILEGE APPLIED TO ENTITIES AND INDIVIDUALS.....	219
– DISSEMINATION OF A WRITTEN REPORT BY COUNSEL.....	219
Notices to Employees as a Result of an Investigation Against a Financial Institution.....	220
Interviewing Employees as a Result of a Law Enforcement Investigation Against a Financial Institution.....	220
Media Relations.....	220
• <b>AML/CFT Cooperation Between Countries.....</b>	<b>221</b>
FATF Recommendations on Cooperation Between Countries.....	221
International Money Laundering Information Network.....	221
Mutual Legal Assistance Treaties.....	222
Financial Intelligence Units.....	223

## **Chapter 5**

Glossary of Terms .....	229
-------------------------	-----

## **Chapter 6**

Practice Questions .....	261
--------------------------	-----

## **Chapter 7**

Guidance Documents and Reference Materials .....	297
Other Websites With Helpful AML Material .....	300
AML-Related Periodicals .....	301

# About ACAMS

**T**he mission of ACAMS is to advance the professional knowledge, skills and experience of those dedicated to the detection and prevention of money laundering around the world, and to promote the development and implementation of sound anti-money laundering policies and procedures. ACAMS achieves its mission through

- promoting international standards for the detection and prevention of money laundering and terrorist financing;
- educating professionals in private and government organizations about these standards and the strategies and practices required to meet them;
- certifying the achievements of its members; and
- providing networking platforms through which AML/CFT professionals can collaborate with their peers throughout the world.

ACAMS sets professional standards for anti-financial crime practitioners worldwide and offers them career development and networking opportunities. In particular, ACAMS seeks to

- help AML professionals with career enhancement through cutting-edge education, certification and training. ACAMS acts as a forum where professionals can exchange strategies and ideas;
- assist practitioners in developing, implementing and upholding proven, sound AML practices and procedures; and
- help financial and non-financial institutions identify and locate individuals with the Certified Anti-Money Laundering (CAMS) designation in the rapidly expanding AML field.

## ABOUT THE CAMS DESIGNATION

As money laundering and terrorist financing threaten financial and nonfinancial institutions and societies as a whole, the challenge and the need to develop experts in preventing and detecting financial crime intensifies. ACAMS is the global leader in responding to that need, having helped standardize AML expertise by creating the CAMS designation.

Internationally recognized, the CAMS credential identifies those who earn it as possessing specialized AML knowledge. AML professionals who earn the CAMS designation position themselves to be leaders in the industry and valuable assets to their organizations.

Congratulations on your decision to pursue the most respected and widely recognized international credential in the AML field. We welcome and invite you to embark on a journey that may lead you to career advancement, international recognition and respect among peers and superiors.

*Read on, study hard and good luck!*

# Chapter 1

## Risks and Methods of Money Laundering and Terrorist Financing

### What is Money Laundering?

---

**M**oney laundering involves taking criminal proceeds and disguising their illegal sources in order to use the funds to perform legal or illegal activities. Simply put, money laundering is the process of making dirty money look clean.

When a criminal activity generates substantial profits, the individual or group involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such profits. Criminals achieve this goal by disguising the source of funds, changing the form or moving the money to a place where it is less likely to attract attention. Criminal activities that lead to money laundering (i.e., predicate crimes) can include illegal arms sales, narcotics trafficking, contraband smuggling and other activities related to organized crime, embezzlement, insider trading, bribery and computer fraud schemes.

Formed in 1989, the Financial Action Task Force (FATF) is an intergovernmental body comprising the Group of Seven industrialized nations to set standards and foster international action against money laundering. One of FATF's early accomplishments was to dispel the notion that money laundering is only about cash transactions. Through several money laundering typologies exercises, FATF demonstrated that money laundering can be achieved through virtually every medium, financial institution or business.

The United Nations 2000 Convention Against Transnational Organized Crime, also known as the Palermo Convention, defines money laundering as

- the conversion or transfer of property, knowing it is derived from a criminal offense, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to or ownership of property knowing that it is derived from a criminal offense; and
- the acquisition, possession or use of property, knowing at the time of its receipt that it was derived from a criminal offense or from participation in a crime.

An important prerequisite in the definition of money laundering is knowledge. In all three of the bullet points mentioned above, we see the phrase "...knowing that it is derived from a criminal offense," and a broad interpretation of knowing is generally applied. In fact, FATF's 40 Recommendations on Money Laundering and Terrorist Financing and the Fourth European Union Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (2015) state that "the intent and knowledge required to prove the offense of money laundering includes the concept that such a mental state may be inferred from objective factual circumstances."

A number of jurisdictions also use the legal principle of willful blindness in money laundering cases to prove knowledge. Courts define willful blindness as the "deliberate avoidance of knowledge of the facts" or "purposeful indifference" and have held that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.

After the events on September 11, 2001, in October 2001, FATF expanded its mandate to cover the financing of terrorism. Both terrorists and money launderers may use the same methods to move their money in ways to avoid detection, such as structuring payments to avoid reporting and use of underground banking or value transfer systems such as hawala, hundi or fei ch'ien. However, whereas funds destined for money laundering are derived from criminal activities, such as drug trafficking and fraud, terrorist financing may include funds from perfectly legitimate sources. Concealment of funds used for terrorism is primarily designed to hide the purpose for which these funds are used, rather than their source. Terrorist funds may be used for operating expenses, including paying for food, transportation and rent, as well as for the actual material support of terrorist acts. Terrorists, similar to criminal enterprises, covet the secrecy of transactions regarding their destination and purpose.

In February 2012, FATF modified its initial list of recommendations and notes into a new list of 40 recommendations, which include a new recommendation addressing ways to prevent, suppress and disrupt the proliferation of weapons of mass destruction.

## Three Stages in the Money Laundering Cycle

Money laundering often involves a complex series of transactions that are difficult to separate. However, it is common to think of money laundering as occurring in three stages.

**Stage One: Placement**—The physical disposal of cash or other assets derived from criminal activity.

During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos and other legitimate businesses, both domestic and international.

Examples of placement transactions include the following.

- Blending of funds: Commingling of illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into cash-intensive, locally owned restaurant

- Foreign exchange: Purchasing of foreign exchange with illegal funds
- Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements
- Currency smuggling: Cross-border physical movement of cash or monetary instruments
- Loans: Repayment of legitimate loans using laundered cash

**Stage Two: Layering**—The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.

This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to obfuscate the source and ownership of funds.

Examples of layering transactions include

- electronically moving funds from one country to another and dividing them into advanced financial options and/or markets;
- moving funds from one financial institution to another or within accounts at the same institution;
- converting the cash placed into monetary instruments;
- reselling high-value goods and prepaid access/stored value products;
- investing in real estate and other legitimate businesses;
- placing money in stocks, bonds or life insurance products; and
- using shell companies to obscure the ultimate beneficial owner and assets.

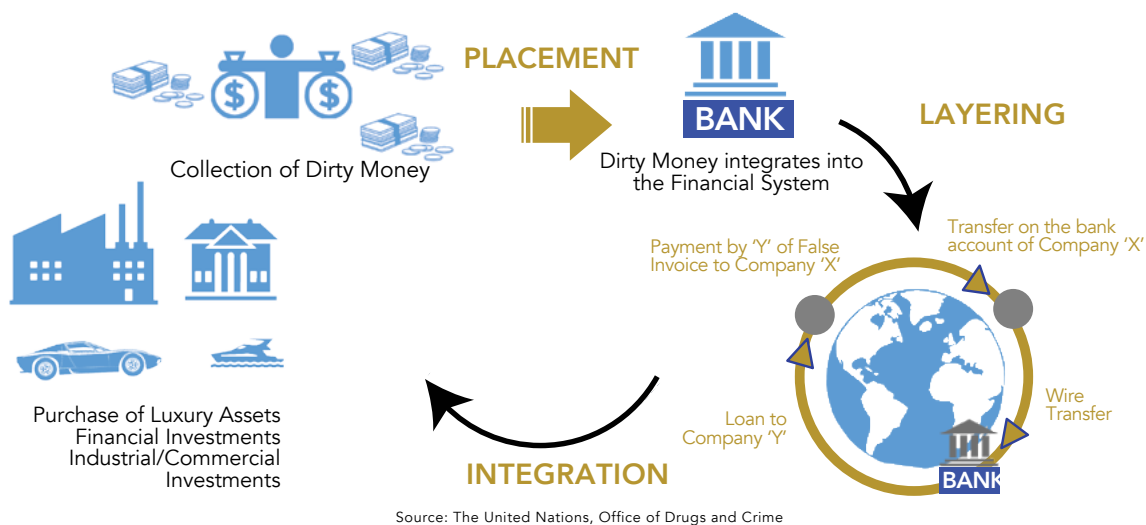
**Stage Three: Integration**—Supplying apparent legitimacy to illicit wealth through the reentry of the funds into the economy in what appears to be normal business or personal transactions.

This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his or her wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets.

Examples of integration transactions include

- purchasing luxury assets, such as property, artwork, jewelry or high-end automobiles; and
- getting into financial arrangements or other ventures where investments can be made in business enterprises.

## Stages of Money Laundering



## The Economic and Social Consequences of Money Laundering

Money laundering is a result of any crime that generates profits for the criminals involved. It knows no boundaries, and jurisdictions where there are weak, ineffective or inadequate anti-money laundering (AML) and counter-terrorism financing (CFT) legislation and regulations are most vulnerable. However, large, well-developed financial centers are also vulnerable to laundering due to the large volumes of transactions that allow the launderer to blend in and the wide range of services that enable the launderer to conduct transactions in a way that is convenient. Because most launderers want to eventually use the proceeds of their crimes, their ultimate intent is to move funds through stable financial systems.

Money laundering has significant economic and social consequences, especially for developing countries and emerging markets. The easy passage of funds from one institution, or relatively facile systems that allow money to be placed without raising any questions, is fertile territory for money launderers. The upholding of legal, professional and ethical standards is critical to the integrity of financial markets.

The potential macroeconomic consequences of unchecked money laundering are as follows.

- **Increased exposure to organized crime and corruption:** Successful money laundering enhances the profitable aspects of criminal activity. When a country is seen as a haven for money laundering, it will attract people who commit crime. Typically, havens for money laundering and terrorist financing have
  - limited numbers of predicate crimes for money laundering (i.e., criminal offenses that may permit a jurisdiction to bring a money laundering charge);
  - limited types of institutions and persons covered by money laundering laws and regulations;

- little to no enforcement of the laws and weak penalties or provisions that make it difficult to confiscate or freeze assets related to money laundering; and
- limited regulatory capacity to effectively monitor and supervise compliance to money laundering and terrorist financing laws and regulations.

If money laundering is prevalent, there is more likely to be corruption. Typically, the penetration of organized crime groups in a jurisdiction is directly linked to public and private sector corruption. Criminals may try to bribe government officials, lawyers and employees of financial or nonfinancial institutions so that they can continue to run their criminal businesses.

In countries with weaker laws and enforcement, it is corruption that triggers money laundering. It also leads to increases in the use of bribery in financial institutions, amongst lawyers and accountants, in the legislature, in enforcement agencies, with police and supervisory authorities, and even with courts and prosecutors.

A comprehensive AML/CFT framework, on the other hand, helps curb criminal activities, eliminates profits from such activities and discourages criminals from operating in a country especially where law is enforced fully and proceeds from crime are confiscated.

### *Case Study*

A U.S. National Security Council report in 2001 found that Russian organizations were taking advantage of Israel's large Russian immigrant community to illegally produce compact discs or CDs and launder the proceeds. Israel gained a reputation as being "good for money laundering" amongst Russian gangsters. Israeli police estimated that more than \$4 billion of dirty money poured into Israel, others estimated it at about \$20 billion. These criminal gangs bought large parcels of land in impoverished development towns, taking over everything from local charities to the town hall, even handpicking several candidates for local and national offices. This further entrenched the gangsters, ensuring they got the benefit of policies and protection from authorities.

- **Undermining the legitimate private sector:** One of the most serious microeconomic effects of money laundering is felt in the private sector.

Money launderers are known to use front companies: businesses that appear legitimate and engage in legitimate business but are in fact controlled by criminals who commingle the proceeds of illicit activity with legitimate funds to hide the ill-gotten gains. These front companies have a competitive advantage over legitimate firms because they have access to substantial illicit funds, allowing them to subsidize products and services sold at below-market rates. This makes it difficult for legitimate businesses to compete against front companies. Clearly, the management principles of these criminal enterprises are not consistent with traditional free market principles, which results in further negative macroeconomic effects.

Finally, by using front companies and other investments in legitimate companies, money laundering proceeds can be used to control whole industries or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxes, thus depriving the country of revenue.

- **Weakening financial institutions:** Money laundering and terrorist financing can harm the soundness of a country's financial sector. They can negatively affect the stability of individual banks or other financial institutions, such as securities firms and insurance companies. Criminal activity has been associated with a number of bank failures around the globe, including the closures of the first Internet bank, European Union Bank, and Riggs Bank. The establishment and maintenance of an effective AML/CFT program is usually part of a financial institution's charter to operate; noncompliance can result not only in significant civil money penalties but also in the loss of its charter.
- **Dampening effect on foreign investments:** Although developing economies cannot afford to be too selective about the sources of capital they attract, there is a dampening effect on foreign direct investment when a country's commercial and financial sectors are perceived to be compromised and subject to the influence of organized crime. To maintain a business-friendly environment these impedances have to be weeded out.
- **Loss of control of, or mistakes in, decisions regarding economic policy:** Due to the large amounts of money involved in the money laundering process, in some emerging market countries these illicit proceeds may dwarf government budgets. This can result in the loss of control of economic policy by governments or in policy mistakes due to measurement errors in macroeconomic statistics.

Money laundering can adversely affect currencies and interest rates as launderers reinvest funds where their schemes are less likely to be detected, rather than where rates of return are higher. Volatility in exchange and interest rates due to unanticipated cross-border transfers of funds can also be seen. To the extent that money demand appears to shift from one country to another because of money laundering—resulting in misleading monetary data—it will have adverse consequences for interest and exchange rate volatility. This is particularly true in economies based on the U.S. dollar, as the tracking of monetary aggregates becomes more uncertain. Last, money laundering can increase the threat of monetary instability due to the misallocation of resources from artificial distortions in asset and commodity prices.

- **Economic distortion and instability:** Money launderers are not primarily interested in profit generation from their investments but rather in protecting their proceeds and hiding the illegal origin of the funds. Thus, they invest their money in activities that are not necessarily economically beneficial to the country where the funds are located. Furthermore, to the extent that money laundering and financial crime redirect funds from sound investments to low-quality investments that hide their origin, economic growth can suffer.
- **Loss of tax revenue:** Of the underlying forms of illegal activity, tax evasion is, perhaps, the one with the most obvious macroeconomic impact. Money laundering diminishes government tax revenue and, therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case.

A government revenue deficit is at the center of economic difficulties in many countries, and correcting it is the primary focus of most economic stabilization programs. The International Monetary Fund (IMF) has been involved in efforts to improve the tax collection capabilities of its member countries and the Organization for Economic Cooperation and Development (OECD) has been instrumental in moving many jurisdictions towards tax transparency.

- **Risks to privatization efforts:** Money laundering threatens the efforts of many states trying to introduce reforms into their economies through the privatization of state-owned properties such as land, resources or enterprises. Sometimes linked with corruption or inside deals, a government may award a state privatization tender to a criminal organization potentially at an economic loss to the public. Moreover, while privatization initiatives are often economically beneficial, they can also serve as a vehicle to launder funds. In the past, criminals have been able to purchase ports, resorts, casinos and other state properties to hide their illicit proceeds and to further their criminal activities.
- **Reputation risk for the country:** A reputation as a money laundering or terrorist financing haven can harm development and economic growth in a country. It diminishes legitimate global opportunities because foreign financial institutions find the extra scrutiny involved in working with institutions in money laundering havens is too expensive.

Legitimate businesses located in money laundering havens may also suffer from reduced access to markets (or may have to pay more to have access) due to extra scrutiny of ownership and control systems. Once a country's financial reputation is damaged, reviving it is very difficult and requires significant resources to rectify a problem that could have been prevented with proper anti-money laundering controls. Other effects include specific countermeasures that can be taken by international organizations and other countries and reduced eligibility for governmental assistance.

- **Risk of international sanctions:** In order to protect the financial system from money laundering and terrorist financing, the United States, the United Nations, the European Union and other governing bodies may impose sanctions against foreign countries, entities or individuals, terrorists and terrorist groups, drug traffickers and other security threats. In the United States, the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions.

Countries can be subject to comprehensive or targeted sanctions. Comprehensive sanctions prohibit virtually all transactions with a specific country. Targeted sanctions prohibit transactions with specified industries, entities or individuals listed on OFAC's Specially Designated Nationals and Blocked Parties List. Failure to comply may result in criminal and civil penalties. FATF also maintains a list of jurisdictions identified as high-risk and noncooperative, whose AML/CFT regimes have strategic deficiencies and are not at international standards. As a result, FATF calls on its members to implement countermeasures against the jurisdiction, such as financial institutions applying enhanced due diligence to business relationships and transactions with natural and legal persons from the identified jurisdiction in an attempt to persuade the jurisdiction to improve its AML/CFT regime.

- **Social costs:** Significant social costs and risks are associated with money laundering. Money laundering is integral to maintaining the profitability of crime. It also enables drug traffickers, smugglers and other criminals to expand their operations. This drives up the cost of government expenses and budgets due to the need for increased law enforcement and other expenditures (e.g., increased healthcare costs for treating drug addicts) to combat the serious consequences that result.

Financial institutions that rely on the proceeds of crime face great challenges in adequately managing their assets, liabilities and operations, as well as in attracting legitimate clients. They also risk being excluded from the international financial system. The adverse consequences of money laundering are reputational, operational, legal and concentration risks and include

- loss of profitable business;
  - liquidity problems through withdrawal of funds;
  - termination of correspondent banking facilities;
  - investigation costs and fines;
  - asset seizures;
  - loan losses; and
  - reduced stock value of financial institutions.
- **Reputational risk:** The potential is that adverse publicity regarding an organization's business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the organization. As an example, reputational risk for a bank represents the potential that borrowers, depositors and investors might stop doing business with the bank because of a money laundering scandal.

The loss of high-quality borrowers reduces profitable loans and increases the risk of the overall loan portfolio. Depositors may withdraw their funds. Moreover, funds placed on deposit with a bank may not be reliable as a source of funding once depositors learn that the bank may not be stable. Depositors may be more willing to incur large penalties rather than leave their funds in a questionable bank, resulting in unanticipated withdrawals, causing potential liquidity problems.
  - **Operational risk:** The potential for loss results from inadequate internal processes, personnel or systems or from external events. Such losses can occur when institutions incur reduced or terminated inter-bank or correspondent banking services or an increased cost for these services. Increased borrowing or funding costs are also a component of operational risk.
  - **Legal risk:** There is potential for lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an organization, or even the closure of the organization. For instance, legitimate customers may become victims of a financial crime, lose money and sue the financial institution for reimbursement. There may be investigations conducted by regulators and/or law enforcement authorities, resulting in increased costs, as well as fines and other penalties. Also, certain contracts may be unenforceable due to fraud on the part of the criminal customer.

- **Concentration risk:** The potential for loss results from too much credit or loan exposure to one borrower or group of borrowers. Regulations usually restrict a bank's exposure to a single borrower or group of related borrowers. Lack of knowledge about a particular customer or who is behind the customer, or what the customer's relationship is to other borrowers, can place a bank at risk in this regard. This is particularly a concern where there are related counterparties, connected borrowers and a common source of income or assets for repayment. Loan losses can also result, of course, from unenforceable contracts and contracts made with fictitious persons.

For these reasons, international bodies have issued statements such as the Basel Committee on Banking Supervision's 2014 guidelines on the *Sound Management of Risks Related to Money Laundering and Financing of Terrorism* and FATF's *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*.

## **AML/CFT Compliance Programs and Individual Accountability**

---

In the past several years, guidance has been issued and laws have been passed seeking individual accountability at the senior levels of regulated financial institutions that have contributed to deficiencies in AML and sanctions compliance programs.

In 2014, the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of the Treasury and the United States' Financial Intelligence Unit (FIU) issued an advisory to financial institutions reminding them to maintain a strong culture of compliance and that the entire staff is responsible for AML/CFT compliance. This advisory was followed in 2015 by a memorandum on "Individual Accountability for Corporate Wrongdoing," from the U.S. Department of Justice's Deputy Attorney General, Sally Quillian Yates.

The Yates Memo, as it is often referred to, reminds prosecutors that criminal and civil investigations into corporate misconduct should also focus on individuals who perpetrated the wrongdoing. Further, it notes that the resolution of a corporate case does not provide protection to individuals from criminal or civil liability. Although the Yates Memo does not specifically address AML/CFT compliance, recent enforcement actions issued by U.S. regulators against financial institutions illustrate a continued focus on AML/CFT compliance deficiencies.

In the United Kingdom, the Financial Conduct Authority (FCA) published final rules for the Senior Managers Regime (2015), which is designed to improve individual accountability within the banking sector. In relation to financial crime, the Senior Managers Regime requires a financial institution to give explicit responsibility to a senior manager, such as an executive-level Money Laundering Reporting Officer (MLRO), for ensuring that the institution's efforts to combat financial crime are effectively designed and implemented. The senior manager is personally accountable for any misconduct that falls within the institution's AML/CFT regime.

Finally, on June 30, 2016, the New York State Department of Financial Services (DFS) issued a Final Rule requiring regulated institutions to maintain "Transaction Monitoring and Filtering Programs" reasonably designed to

- (i) monitor transactions after their execution for compliance with the Bank Secrecy Act (BSA) and anti-money laundering (AML) laws and regulations, including suspicious activity reporting requirements; and
- (ii) prevent unlawful transactions with targets of economic sanctions administered by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC).

This Final Rule, which went into effect on January 1, 2017, also requires regulated institutions' boards of directors or senior officer(s) to make annual certifications to the DFS confirming that they have taken all steps necessary to comply with transaction monitoring and filtering program requirements.

Although the law may seem New York-specific on its face, numerous foreign banks fall within the law because they operate in New York. Specifically, the law covers banks, trust companies, private bankers, savings banks and savings and loan associations chartered pursuant to the New York Banking Law and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York. Moreover, the law also applies to non-bank financial institutions with a Banking Law license, such as check cashers and money transmitters.

#### Case Study

From 2003 to 2008, Thomas Haider served as the Chief Compliance Officer for MoneyGram, a money services business (MSB) specializing in money transfers. As part of his responsibilities, Mr. Haider was responsible for ensuring that MoneyGram had an effective AML/CFT program that requires timely reporting of suspicious transactions. He was also in charge of MoneyGram's Fraud Department.

During that time, there were thousands of complaints placed by customers who reported that they were victims of lottery or prepayment fraud and instructed to remit money to fraudsters via MoneyGram agents in the United States and Canada. Although receiving a wealth of information from complainants, Mr. Haider and MoneyGram's Fraud Department did not conduct an investigation of the complaints or the outlets from where the complaints were generated. An investigation would have allowed Mr. Haider to suspend or terminate any agent participating in the illegal activity.

According to a December 2014 FinCEN assessment of civil penalty, Mr. Haider failed to implement an appropriate AML program, conduct effective audits or terminate known high-risk agents. As a result of FinCEN's investigation, Mr. Haider was removed from his employment at MoneyGram in 2008 and was individually assessed a \$1 million civil money penalty in 2014. FinCEN also sought to bar Mr. Haider from working in the financial services industry.

## **Methods of Money Laundering**

---

Money laundering is an ever-evolving activity; it must be continuously monitored in all its various forms in order for measures against it to be timely and effective. Illicit money can move through numerous different commercial channels, including products such as checking, savings and brokerage accounts; loans; wires and transfers or through financial intermediaries, such as trusts and company service providers, securities dealers, banks and money services businesses.

A money launderer will seek to operate in and around the financial system in a manner that best fits the execution of the scheme to launder funds. As many governments around the world have implemented AML obligations for the banking sector, a shift in laundering activity into the nonbank financial sector and to nonfinancial businesses and professions has risen.

FATF and FATF-style regional bodies publish periodic typology reports to “monitor changes and better understand the underlying mechanisms of money laundering and terrorist financing.” The objective is to report on some of the “key methods and trends in these areas” and to also make certain that the FATF 40 Recommendations remain effective and relevant. In this chapter, we will refer often to these typologies because they give good examples of how money can be laundered through different methods and in different settings.

## **Banks and Other Depository Institutions**

---

Banks have historically been and continue to be important mechanisms in all three stages of money laundering. Below are some special areas of interest and concern for money laundering through banks and other depository institutions.

### **ELECTRONIC TRANSFERS OF FUNDS**

An electronic transfer of funds is any transfer of funds that is initiated by electronic means, such as an Automated Clearing House (ACH) computer, an automated teller machine (ATM), electronic terminals, mobile telephones, telephones or magnetic tapes. It can happen within a country or across borders, and trillions of dollars are transferred in millions of transactions each day, because it is one of the fastest ways to move money.

Systems such as the Federal Reserve Wire Network (Fedwire), the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and the Clearing House Interbank Payments System (CHIPS) move millions of wires or transfer messages daily. As such, illicit fund transfers can be easily hidden among the millions of legitimate transfers that occur each day. For example, money launderers may initiate unauthorized domestic or international electronic transfers of funds—such as ACH debits or by making cash advances on a stolen credit card—and place the funds into an account established to receive the transfers. Another example is stealing credit cards and using the funds to purchase merchandise that can be resold to provide the criminal with cash.

Money launderers also use electronic transfers of funds in the second stage of the laundering process, the layering stage. The goal is to move the funds from one account to another, from one bank to another and from one jurisdiction to another with each layer of transactions—making it more difficult for law enforcement and investigative agencies to trace the origin of the funds.

To avoid detection in either stage, the money launderer may take basic precautions, such as varying the amounts sent, keeping them relatively small and under reporting thresholds, and, where possible, using reputable organizations.

The processes in place to verify the electronic transfer of funds have been tightened in recent years. Many transaction monitoring software providers have sophisticated algorithms to help detect or trigger alerts that may indicate money laundering or other suspicious activity using electronic transfers of funds. However, no system is foolproof.

Some indicators of money laundering using electronic transfers of funds include the following.

- Funds transfers occur to or from a financial secrecy haven, to or from a high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explanation or apparent reason.
- Many small, incoming transfers of funds are received or deposits are made using checks and money orders. Upon credit to the account, all or most of the transfers or deposits are wired to another account in a different geographic location in a manner inconsistent with the customer's business or history.
- Funds activity is unexplained, repetitive or shows unusual patterns.
- Payments or receipts are received that have no apparent link to legitimate contracts, goods or services.
- Funds transfers are sent or received from the same person to or from different accounts.

## REMOTE DEPOSIT CAPTURE

Remote Deposit Capture (RDC) is a product offered by banks that allows customers to scan a check and transmit an electronic image to the bank for deposit. This offers increased convenience for customers because they no longer need to make a trip to the bank or an ATM to deposit checks. Previously, this was offered only via specialized scanners to commercial customers, but now many banks allow individuals to deposit pictures of checks taken with mobile phones. RDC decreases the cost to process checks for banks and is part of a gradual transition away from paper-based transactions. RDC is also increasingly used in correspondent banking for the same reasons, because it streamlines the deposit and clearing process. Correspondent banking is the provision of banking services by one bank to another bank.

The convenience provided by RDC lends itself to potential abuse by money launderers because they no longer need to go into the bank and risk detection. Once a money launderer has RDC capabilities, he or she can move checks with ease through an account. It might even be possible to set up multiple imaging devices (e.g., multiple scanners and multiple permitted mobile phones) that will enable a money launderer to allow others to process checks through the system. It might even be possible for the money launderer to have someone else set up the account and provide him or her with the ability to deposit checks. Without proper controls, RDC can also be misused to facilitate violations of sanctions requirements (e.g., processing transactions in a sanctioned country).

Although RDC can be used for money laundering, the more prominent risk relates to fraud. Because RDC minimizes human intervention in reviewing cleared items, the ability to identify potential fraud indicators, such as an altered check or multiple deposits of the same item, decreases. Often, the resulting fraud is not prevented but rather detected after it has already occurred.

To control the risks associated with RDC, efforts must be made to integrate RDC processing into other controls, such as monitoring and fraud prevention systems. In fact, this integration should occur with any new product offered by a bank. This includes ensuring that items submitted via RDC are reviewed for sequentially numbered checks and money orders without payees; that the total volume of activity processed for an account via RDC is incorporated into the overall transaction monitoring; that appropriate limits are placed on a customer's ability to deposit checks via RDC; that the product is offered to customers to whom it is appropriate; and that appropriate action is taken quickly when fraud is detected via RDC items.

## **CORRESPONDENT BANKING**

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). By establishing multiple correspondent relationships globally, banks can undertake international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence. Large international banks typically act as correspondents for thousands of other banks around the world.

Respondent banks obtain a wide range of services through correspondent relationships, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers of funds, check clearing, payable-through accounts and foreign exchange services.

Before establishing correspondent accounts, banks should be able to answer basic questions about the respondent bank, including who its owners are and the nature of its regulatory oversight. Respondent banks judged to be sound credit risks may be offered a number of credit-related products (e.g., letters of credit and business accounts for credit card transactions). The services offered by a correspondent bank to smaller, less well-known banks may be restricted to noncredit, cash management services.

Correspondent banking is vulnerable to money laundering for two main reasons.

1. By their nature, correspondent banking relationships create a situation in which a financial institution carries out financial transactions on behalf of customers of another institution. This indirect relationship means that the correspondent bank provides services for individuals or entities for which it has neither verified the identities nor obtained any firsthand knowledge.
2. The amount of money that flows through correspondent accounts can pose a significant threat to financial institutions, because they process large volumes of transactions for their customers' customers. This makes it more difficult to identify suspect transactions, because the financial institution generally does not have the information on the actual parties conducting the transaction to know whether they are unusual.

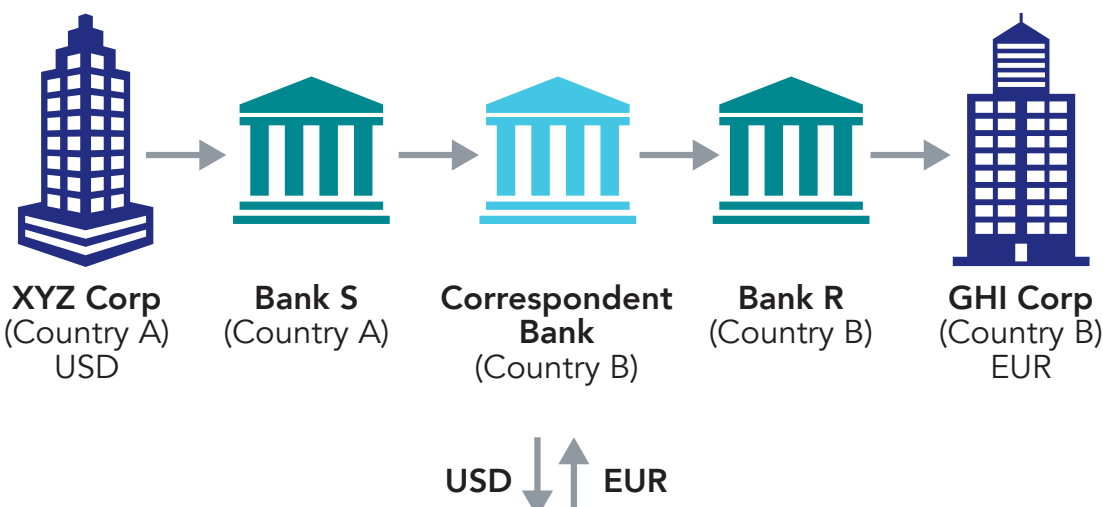
Additional risks incurred by the correspondent bank include: the following.

- Although the correspondent bank may be able to learn what laws govern the respondent bank, determining the degree and effectiveness of the supervisory regime to which the respondent is subject may be much more difficult. This can make it difficult to determine the level of risk associated with developing a relationship with a respondent bank.
- Determining the effectiveness of the respondent bank's AML controls can also be a challenge. Although requesting compliance questionnaires will provide some comfort, the correspondent bank is still very reliant on the respondent doing its own due diligence on the customers it allows to use the correspondent account.
- Some banks offering correspondent facilities may not ask their respondents about the extent to which they offer such facilities to other institutions, a practice known as nesting. This means the correspondent bank is even further removed from knowing the identities or business activity of these subrespondents or even the types of financial services provided.

### Case Study

In March 2015, U.S. regulators closed Florida-based North Dade Community Development Federal Credit Union for willful violations of the USA PATRIOT Act, the Bank Secrecy Act (BSA) and provisions to its credit union charter and bylaws. The credit union had only one office staffed by five people. The credit union's purpose was to provide basic financial services to its members from the local community. However, FinCEN observed that the credit union had correspondent banking relationships with money services businesses (MSBs) in high-risk jurisdictions in Latin America and the Middle East. In 2013, the credit union processed approximately \$55 million in cash orders, \$1 billion in outgoing wire transfers, \$5 million in returned checks and \$985 million in remote deposit capture for its MSB clients. FinCEN stated that these funds could have been linked to money laundering or supporting terrorist organizations. Moreover, FinCEN identified the activity was not expected business behavior of a small credit union like North Dade and led to substantial AML/CFT compliance failures and violations, including willfully violating its BSA program, record-keeping, reporting and requirements. As a result, North Dade consented to a \$300,000 civil money penalty. Subsequently, the National Credit Union Association (NCUA), the banks' financial regulator, liquidated North Dade after determining it had violated various provisions of its charter, bylaws and federal regulations.

## Correspondent Banking Transaction Example (Single Correspondent)



### PAYABLE THROUGH ACCOUNTS

In some correspondent relationships, the respondent bank's customers are permitted to conduct their own transactions—including sending wire transfers, making and withdrawing deposits and maintaining checking accounts—through the respondent bank's correspondent account without first clearing the transactions through the respondent bank. Those arrangements are called payable-through accounts (PTAs). In a traditional correspondent relationship, the respondent bank will take orders from its customers and pass them on to the correspondent bank. In these cases, the respondent bank has the ability to perform some level of oversight prior to executing the transaction. PTAs differ from normal correspondent accounts in that the foreign bank's customers have the ability to directly control funds at the correspondent bank.

PTAs can have a virtually unlimited number of subaccount holders, including individuals, commercial businesses, finance companies, exchange houses or casas de cambio and even other foreign banks. The services offered to subaccount holders and the terms of the PTAs are specified in the agreement signed by the correspondent and the respondent banks.

PTAs held in the names of respondent banks often involve checks encoded with the bank's account number and a numeric code to identify the subaccount, which is the account of the respondent bank's customer. Sometimes, however, the subaccount holders are not identified to the correspondent bank.

Elements of a PTA relationship that can threaten the correspondent bank's money laundering defenses include the following.

- PTAs with foreign institutions licensed in offshore financial service centers with weak or nascent bank supervision and licensing laws

- PTA arrangements where the correspondent bank regards the respondent bank as its sole customer and fails to apply its Customer Due Diligence policies and procedures to the customers of the respondent bank
- PTA arrangements in which subaccount holders have currency deposit and withdrawal privileges
- PTAs used in conjunction with a subsidiary, representative or other office of the respondent bank, which may enable the respondent bank to offer the same services as a branch without being subject to supervision

### Case Study

Lombard Bank, a bank licensed by the South Pacific island of Vanuatu, opened a payable-through account at American Express Bank International (AEBI) in Miami. The Vanuatu bank was permitted to have multiple authorized signatures on the account.

Lombard customers had no relationship with AEBI. However, the bank offered its Central American customers virtually full banking services through its payable-through account at AEBI. They were even given checkbooks allowing them to deposit and withdraw funds from Lombard's payable-through account.

Lombard's PTA subaccount holders would bring cash deposits to Lombard representatives in four Central American countries. Lombard couriers would then transport the cash to its Miami affiliate, Lombard Credit Corporation, for deposit in the payable-through account at AEBI. Lombard customers also brought cash to the Lombard office in Miami, which was located in the same building as AEBI. That cash was also deposited in the payable-through account at AEBI. Over the 2 years ending in June 1993, as much as \$200,000 in cash was received by Lombard's Miami affiliate on 104 occasions. As a result, AEBI lacked any visibility into the source of the cash being deposited by Lombard's customers' into the PTA at AEBI, raising significant AML/CFT compliance concerns with know your customer, due diligence and record-keeping and regulatory filing requirements.

## **CONCENTRATION ACCOUNTS**

Concentration accounts are internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the bank, usually on the same day. They do this by aggregating funds from several locations into one centralized account (i.e., the concentration account) and are also known as special-use, omnibus, settlement, suspense, intraday, sweep or collection accounts. Concentration accounts are frequently used to facilitate transactions for private banking, trust and custody accounts, funds transfers and international affiliates.

Money laundering risks can arise in concentration accounts if the customer-identifying information, such as name, transaction amount and account number, is separated from the financial transaction. If separation occurs, the audit trail is lost, and accounts may be misused or administered improperly.

Banks that use concentration accounts should implement adequate policies, procedures and processes covering operation and record-keeping for these accounts, including

- requiring dual signatures on general ledger tickets;

- prohibiting direct customer access to concentration accounts;
- capturing customer transactions in the customer's account statements;
- prohibiting customers' knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts;
- retaining appropriate transaction and customer-identifying information;
- reconciling accounts frequently by an individual who is independent from the transactions;
- establishing a timely discrepancy resolution process; and
- identifying and monitoring recurring customer names.

## PRIVATE BANKING

Private banking is an extremely lucrative, competitive and global industry. Since the 2008 financial crisis, U.S. and EU officials have placed greater scrutiny on private banks and their services, particularly in tax planning strategies.

Private banking provides highly personalized and confidential products and services to wealthy clients at fees that are often based on "assets under management." Private banking often operates semiautonomously from other parts of a bank.

Fierce competition among private bankers for the high net-worth individuals who are their main clientele has given rise to the need for tighter government controls worldwide. Competition brings increased pressures on the relationship managers and the marketing officers to obtain new clients, to increase their assets under management and to contribute a greater percentage to the net income of their organizations. Plus, the compensation paid to most relationship managers in private banking is based largely on the assets under management that they bring to their institutions.

The following factors may contribute to the vulnerabilities of private banking with regard to money laundering.

- Perceived high profitability
- Intense competition
- Powerful clientele
- The high level of confidentiality associated with private banking
- The close trust developed between relationship managers and their clients
- Commission-based compensation for relationship managers
- A culture of secrecy and discretion developed by the relationship managers for their clients
- The relationship managers becoming client advocates to protect their clients
- Use of private investment companies by clients to reduce transparency of the beneficial owner
- Clients maintaining personal and business wealth in numerous jurisdictions

- Clients being able to utilize and control numerous legal entities for personal and family estate planning purposes

### *Case Study*

Two private bankers formerly employed by American Express Bank International were convicted of money laundering for the Mexican drug cartel of Juan Garcia Abrego in 1994. For their role in the criminal activity, they cited the competitive nature of the field, the method of compensation and “the pressure on international bankers to recruit new clients and the concomitant professional and monetary success that comes to those who are able to produce.”

Also in the United States, Riggs Bank maintained a close relationship with Augusto Pinochet, the former president of Chile. This relationship with Pinochet included flying to and from Chile on his private jet and taking hundreds of thousands of dollars’ worth of cashier’s checks to Pinochet. These funds were later found to be the proceeds of corruption. Riggs also facilitated the movement of money through real estate transactions that appeared to be structured in such a way as to avoid linking them to Pinochet. In May 2004, Riggs Bank, which was a well-respected bank founded in the 1800s, was fined \$25 million for violations of the U.S. Bank Secrecy Act. Subsequently, in 2005, Riggs pleaded guilty to a federal criminal violation of the Bank Secrecy Act by a repeated and systemic failure to accurately report suspicious monetary transactions associated with bank accounts owned and controlled by Augusto Pinochet of Chile and by the government of Equatorial Guinea. Riggs was fined \$16 million, the largest criminal penalty ever imposed on a bank Riggs’s size. As a result, Riggs also voluntarily closed its Embassy Banking and International Private Banking Divisions. Subsequently, Riggs was acquired by another bank and the Riggs name was retired.

## **USE OF PRIVATE INVESTMENT COMPANIES IN PRIVATE BANKING**

In offshore or international financial centers, private banking customers are often nonresidents, meaning they conduct their banking in a country outside the one in which they reside. Their assets may move overseas where they are held in the name of corporate vehicles like private investment companies (PICs) established in secrecy havens. PICs are corporations established by individual bank customers and others in offshore jurisdictions to hold assets. They are shell companies formed to maintain clients’ confidentiality and for various tax- or trust-related reasons. They have been an element of many high-profile laundering cases in recent years because they are excellent laundering vehicles.

The secrecy laws of the offshore havens where PICs are often established can conceal the true identity of their beneficial owners. As an additional layer of secrecy, some PICs are established by company formation agents with nominee directors who hold title to the company for the benefit of individuals. These beneficial owners may remain undisclosed and sometimes subject to an attorney-client privilege or other similar legal safeguards. Many private banks establish PICs for their clients, often through an affiliated trust company in an offshore secrecy haven. Illicit actors may establish complex shell company networks where a company registered in one offshore jurisdiction may be linked to companies or accounts in other jurisdictions.

### Case Study

In 2014, Israeli-based Bank Leumi admitted that it assisted more than 1,500 U.S. taxpayers in hiding their assets in Bank Leumi's offshore affiliates in Switzerland and Luxembourg. According to reports, for several years Bank Leumi sent private bankers to the United States to meet with its U.S. clients to discuss their offshore portfolio and tax mitigation strategies. As part of this, the bank assisted in organizing nominee corporate entities registered in Belize and other offshore jurisdictions to hide their clients' private offshore accounts and maintained several U.S. clients' accounts under assumed names or numbered accounts. Bank Leumi also provided "hold mail" services and offered loans to its U.S. clients that were collateralized by their offshore assets that were not declared to U.S. tax authorities. As a result of the settlement, Bank Leumi was assessed \$270 million in fines and the bank was ordered to cease providing private banking and investment services for all U.S. clients or accounts with U.S. beneficial owners. This settlement led to Bank Leumi selling its affiliates Bank Leumi Private Bank and Bank Leumi (Luxembourg).

## POLITICALLY EXPOSED PERSONS

According to FATF's *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012), there are two types of politically exposed persons (PEPs).

- **Foreign PEPs:** Individuals who are or have been entrusted with prominent public functions by a foreign country (e.g., heads of state or of government; senior politicians; senior government, judicial or military officials; senior executives of state-owned corporations and important political party officials).
- **Domestic PEPs:** Individuals who are or have been entrusted domestically with prominent public functions (e.g., heads of state or of government; senior politicians; senior government, judicial or military officials; senior executives of state-owned corporations and important political party officials).

PEPs have been the source of problems for several financial institutions, as the examples below show.

- **Mario Villanueva:** The corrupt governor of the Mexican state of Quintana Roo facilitated the smuggling of 200 tons of cocaine into the United States, according to the U.S. Drug Enforcement Agency (DEA). For 5 years, until 2001, he maintained private banking accounts at Lehman Brothers containing approximately \$20 million that the DEA alleged he had received as bribes from Mexican drug traffickers.
- **The Riggs Bank** case revealed a web of transactions, involving hundreds of millions of dollars, that the bank had facilitated over many years for dictators on two continents, including Augusto Pinochet of Chile and Teodoro Obiang of Equatorial Guinea. The accounts formed part of the embassy banking portfolio that was the bank's specialty product for decades.

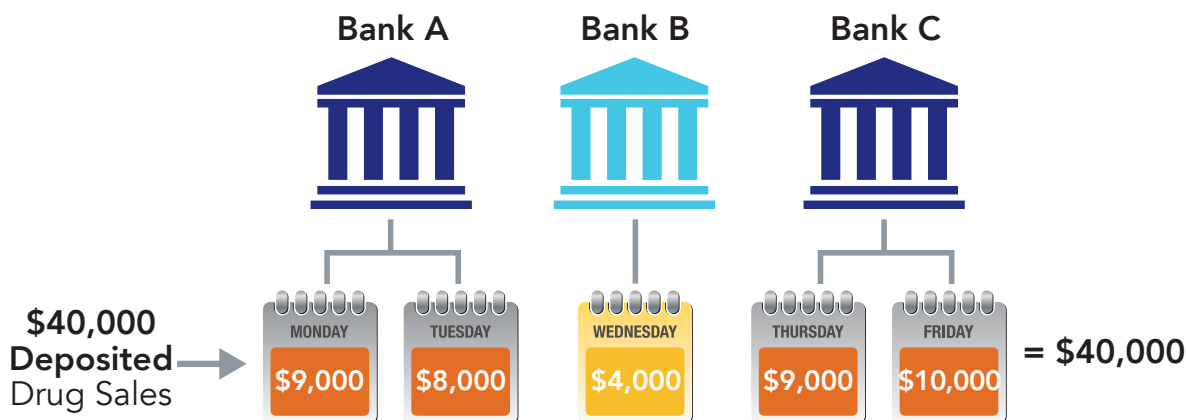
- **Vladimiro Montesinos:** the former head of Peru's Intelligence Service, and chief advisor of former Peruvian president Alberto Fujimori, had accounts at The Bank of New York in New York City, which held the proceeds from substantial bribes from drug traffickers. Other institutions, such as American Express Bank International, Bank of America, Barclays and UBS AG in New York, also held accounts for Montesinos. In addition, he used shell companies to facilitate embezzlement, gun running, drug trafficking and money laundering in excess of \$400 million globally.
- **Arnoldo Aleman and Byron Jerez:** The former president and former tax commissioner of Nicaragua maintained accounts at Terrabank N.A. in Miami, through which they bought millions of dollars of certificates of deposit and condominiums in South Florida, allegedly with the proceeds of corruption.
- **Pavel Lazarenko:** The former prime minister of Ukraine had accounts in San Francisco at Bank of America, Commercial Bank, Pacific Bank, Westamerica Bank and various securities firms, including Fleet Boston, Robertson & Stephens, Hambrecht & Quist and Merrill Lynch, where millions of dollars he allegedly extorted as head of state of Ukraine were held.
- **Colonel Victor Venero Garrido:** A Peruvian army officer, whom the U.S. FBI described as the "most trusted bag/straw man" of Vladimiro Montesinos, maintained accounts at Citibank in Miami and Northern Trust in California that allegedly held more than \$15 million in bribes and extortion proceeds.
- **Mario Ruiz Massieu:** The former deputy attorney general of Mexico in charge of drug trafficking prosecutions maintained a private banking account at Texas Commerce Bank in Houston in the mid-1990s, where he deposited drug traffickers' bribes of \$9 million in currency over a 13-month period.
- **Omar Bongo:** The president of Gabon in Central Africa for 41 years until his death in 2009, Bongo used offshore shell companies to move over \$100 million in suspected funds through private bank accounts, including providing large amounts of cash to family members for his benefit.

## STRUCTURING

Designing a transaction to evade triggering a reporting or record keeping requirement is called *structuring*. Structuring is possibly the most commonly known money laundering method. It is a crime in many countries and must be reported by filing a suspicious transaction report. The individuals engaged in structuring may be runners hired by the launderers. These individuals go from bank to bank depositing cash and purchasing monetary instruments in amounts under reporting thresholds.

Structuring can be done in many settings or industries, including banking, money services businesses and casinos. A common technique involved in structuring is called *smurfing*, which involves multiple individuals making multiple cash deposits and/or buying multiple monetary instruments or bank drafts in amounts under the reporting threshold in an attempt to evade detection.

## Cash Structuring Example



Structuring remains one of the most common reported forms of unusual activity. Below are some well-known examples.

- **A customer breaks a large transaction into two or more smaller ones.**

Henri wants to conduct a transaction involving \$18,000 in cash. However, knowing that depositing it all at once would exceed the cash reporting threshold of \$10,000 in cash and would trigger the filing of a currency transaction report, he goes to three different banks and deposits \$6,000 in each.

- **A large transaction is broken into two or more smaller transactions conducted by two or more people.**

Jennifer wants to send a \$5,000 money transfer, but knowing that in her country there is a threshold of \$3,000 for the recording of funds transfers, she sends a \$2,500 money transfer and asks her friend to send another \$2,500 money transfer.

- **A wealthy Chinese man sends his fortune across to London.**

Mr. Lee sends his gained wealth of 1 million pounds in sums of \$40,000 via friends and business contacts to a British bank in London. The reason why he is not sending it to his own bank account in London is that the Chinese government has currency controls in place for transactions over \$50,000 abroad.

### Case Study

Structuring has been around for a long time, as is evidenced by this case from the early 1980s. Although the case is old, the method continues to be used: breaking down transactions below the reporting threshold.

Isaac Kattan was a travel agent and businessman. Kattan allegedly laundered an estimated \$500 million per year in drug money, all of it in cash. Couriers from a number of cities would visit him in his apartment, leaving boxes and suitcases full of money. The bagmen were messengers from narcotics distributors. The money was payment to their suppliers in Colombia. One of Kattan's

favorite places for making deposits was The Great American Bank of Dade County. Officials in the bank were bribed to accept his massive deposits without filing currency transaction reports (CTRs).

Hernan Botero allegedly had a similar but smaller operation to Kattan's. He laundered only about \$100 million per year from cocaine deals out of his home near Palm Beach. Botero was indicted in the United States and testimony in federal court showed he had bribed officers and employees of the Landmark Bank in Plantation, Florida, to accept his deposits. The money was brought in to the bank almost daily by Botero front companies. From Landmark, the money was transferred to the Miami accounts of Colombian banks. From there, it was a simple matter to wire the money to banks in Colombia. Kattan and Botero were sentenced to 30-year terms in federal prison.

Here is how foreign money brokers structure transactions.

1. A structurer, who is acting for a foreign money broker, opens numerous checking accounts in Country A using real and fictitious names. Sometimes the structurer uses identification documents of dead people supplied by the money brokers.
2. With funds supplied by the money brokers, the structurer opens the accounts with inconspicuous amounts, usually in the low four-figures.
3. To allay bank suspicions, the money brokers sometimes deposit extra funds to cover living expenses and to give the accounts an air of legitimacy.
4. Once the accounts are opened, the structurer signs the newly issued checks, leaving the payee, date and amount lines blank.
5. He sends the signed blank checks to the money broker in country B, usually by courier.
6. A structurer may open as many as two dozen checking accounts in this fashion. It is not uncommon for brokers to have more than 20 of these checking accounts in Country A available at any given time.
7. The checking accounts usually accumulate only a few thousand dollars before they are cleared out by checks drawn by the money brokers to pay for exports from Country A to Country B's money brokerage customers.
8. The availability of hundreds of these accounts to Country B's money brokers leaves open the possibility that tens of millions of dollars may pass through them each year.

## MICROSTRUCTURING

Another method of placing large amounts of illicit cash into the financial system is microstructuring. Microstructuring is essentially the same as structuring, except that it is done at a much smaller level. Instead of taking \$18,000 and breaking it into two deposits to evade reporting requirements, the microstructurer breaks it into 20 deposits of approximately \$900 each, making the suspicious activity extremely difficult to detect.

In the case of a Colombian drug cartel, the cash proceeds of U.S. drug sales were deposited into accounts in New York with ATM cards linked to them. The cards were provided to associates in Colombia. Deposits were made on a regular schedule with the Colombian associates withdrawing the funds as they were deposited and providing them to the drug lords. In one case in New York, an individual was trailed by law enforcement authorities as he went from bank to bank in Manhattan. When they stopped him, he had \$165,000 in cash.

Methods of detecting microstructuring include

- the use of counter deposit slips as opposed to preprinted deposit slips;
- frequent activity in an account immediately following the opening of the account with only preliminary and incomplete documentation;
- frequent visits to make cash deposits of nominal amounts that are inconsistent with typical business or personal banking activity;
- cash deposits followed by ATM withdrawals, particularly in higher risk countries; and
- cash deposits made into business accounts by third parties with no apparent connection to the company.

## **Credit Unions and Building Societies**

---

Credit unions, also known as building societies in some jurisdictions, are not-for-profit, member-owned and -operated democratic financial co-operatives.

Credit unions do not have clients or customers; instead they have members who are also owners. Credit unions serve only the financial needs of their members and are governed by a “one member, one vote” philosophy. A member must purchase an initial capital share of the credit union, permitting him or her to access the products and services offered by the credit union. Credit union membership is based on a common bond, a linkage shared by savers and borrowers who belong to a specific community, organization, religion or place of employment.

Credit unions may vary greatly in both size and complexity. Some credit unions may have a few hundred members whereas others may have hundreds of thousands of members with tens of billions of dollars in assets under management. Some credit unions will focus on meeting only a few niche needs of their members, whereas others will offer a full suite of products and services to rival most retail banks.

Most credit unions focus primarily on servicing personal banking relationships from within their community. Depending on their member eligibility model, some may also facilitate memberships for small- to medium-sized corporate and entity account holders, though the credit union may be prohibited from doing so in certain jurisdictions. Generally, credit unions do not participate in trade-based financing, will not facilitate correspondent banking relationships and will not maintain large corporate relationships, particularly those with international banking needs.

In many jurisdictions, credit unions rely on credit union centrals for a variety of services. A credit union central is best defined as a trade association for credit unions; it is owned by its member credit unions and helps to serve many of their financial needs. Services may include those related to capital liquidity; research, training and advocacy with respect to regulatory obligations; shared operational or back-office processes, such as check clearing; and electronic funds transfer (EFT) processing. In general, they help to negotiate shared contracts for common services, allowing many smaller credit unions to leverage economies of scale that they would not otherwise be able to do.

With respect to regulatory requirements and oversight, credit unions operate very similarly to banks in most jurisdictions. They have similar capital, liquidity, risk management, record keeping and reporting obligations as banks, though there may be some minor differences between institutions that are subject to the oversight of regional versus federal regulators and regulations. Because credit unions are included under FATF's definition of a financial institution, national AML/CFT regimes that follow FATF's recommendations treat credit unions similarly to banks.

The United Kingdom's Joint Money Laundering Steering Group (JMLSG) stated in its November 2006 guidance that, although credit unions pose a low money laundering risk due to their smaller average size and fewer products offered, they are still vulnerable to money laundering and terrorist financing schemes. Not surprisingly, the JMLSG found that the more financial services a credit union offers, the higher the potential risk for money laundering, because these credit unions or building societies tend to contain a larger clientele and offer potential criminals a larger range of possible ways to conceal their illicit funds.

In November 2014 guidance by the JMLSG, the group concluded that high-risk transactions include money transfers to third parties, third parties paying in cash for someone else and reluctance to provide identity information when opening an account. And because credit unions typically deal with small amounts and members with very regular behavior, another money laundering indicator given in the guidelines is there are transactions of larger than usual amounts and erratic member behavior.

The JMLSG even advised credit unions to watch for unusual activity in the accounts of children because parents could be trying to use those funds for illicit purposes, thinking such transactions would draw less attention. Examples in the past have shown that even bankrupted companies continued their operations on the bank accounts of children.

## **Nonbank Financial Institutions**

---

### **CREDIT CARD INDUSTRY**

The credit card industry includes

- credit card associations, such as American Express, MasterCard and Visa, which license member banks to issue bankcards, authorize merchants to accept those cards or both;
- issuing banks, which solicit potential customers and issue the credit cards;
- acquiring banks, which process transactions for merchants who accept credit cards; and

- third-party payment processors (TPPP), which contract with issuing or acquiring banks to provide payment processing services to merchants and other business entities, typically initiating transactions on behalf of merchant clients that do not have a direct relationship with the TPPP's financial institution.

Credit card accounts are not likely to be used in the initial placement stage of money laundering because the industry generally restricts cash payments. They are more likely to be used in the layering or integration stages.

### Example

Money launderer Josh prepays his credit card using illicit funds that he has already introduced into the banking system, creating a credit balance on his account. Josh then requests a credit refund, which enables him to further obscure the origin of the funds. This constitutes layering. Josh then uses the illicit money he placed in his bank account and the credit card refund to pay for a new kitchen. Through these steps he has integrated his illicit funds into the financial system.

A money launderer places his ill-gotten funds in accounts at offshore banks and then accesses these funds using credit and debit cards associated with the offshore account. Alternatively, he smuggles the cash out of one country into an offshore jurisdiction with lax regulatory oversight, places the cash in offshore banks and accesses the illicit funds using credit or debit cards.

In a 2002 report called *Extent of Money Laundering through Credit Cards Is Unknown*, the U.S. Government Accountability Office, the Congressional watchdog of the United States, offered the following hypothetical money laundering scenario using credit cards: "Money launderers establish a legitimate business in the U.S. as a 'front' for their illicit activity. They establish a bank account with a U.S.-based bank and obtain credit cards and ATM cards under the name of the 'front business.' Funds from their illicit activities are deposited into the bank account in the United States. While in another country, where their U.S.-based bank has affiliates, they make withdrawals from their U.S. bank account, using credit cards and ATM cards. Money is deposited by one of their cohorts in the U.S. and is transferred to pay off the credit card loan or even prepay the credit card. The bank's online services make it possible to transfer funds between checking and credit card accounts."

## THIRD-PARTY PAYMENT PROCESSORS

Third-party payment processors are generally bank customers that provide payment-processing services to merchants and other business entities and often use their commercial bank accounts to conduct payment processing for their merchant clients. Oftentimes, they are not subject to any AML/CFT requirements.

TPPPs traditionally contracted with U.S. retailers (i.e., merchants) that had physical locations in the United States in order to help collect monies owed by customers. These merchant transactions primarily included credit card payments but also covered Automated Clearing House (ACH) debits and creating and depositing remotely created checks (RCCs) or demand drafts. With the expansion of the Internet, TPPPs may now service a variety of domestic and international merchants, including conventional retail and Internet-based establishments as well as prepaid travel and Internet gaming

enterprises. Considering the expansion of services and the fact that a financial institution maintains a relationship with the TPPP and not the underlying merchant, it becomes difficult for the financial institution to know on whose behalf it is processing a transaction.

The types of merchants that a TPPP provides its payment processing services to can increase the TPPP's vulnerability to money laundering, identity theft, fraud and other illegal activity. For example, TPPPs that provide services to telemarketing, gambling (online, casinos etc.) or Internet merchants and/or process RCCs for these entities may present a higher level risk of risk to a financial institution, because these types of businesses carry a high risk for consumer fraud and money laundering.

Examples of risks posed by TPPP include the following.

- **Multiple financial institution relationships:** The TPPP may maintain relationships at multiple institutions, which hinders a financial institution's ability to see the entire customer relationship. This is done on purpose by TPPPs engaged in suspicious activity to limit the financial institutions' ability to recognize suspicious activity and exit the relationship.
- **Money laundering:** TPPPs can be used by criminals to mask transactions and launder the proceeds of crime. One way to engage in money laundering through a TPPP is to send funds directly to a financial institution from a foreign jurisdiction through an international ACH payment. Given the large number of transactions conducted through a TPPP, this activity may not be identified.
- **High return rates from unauthorized transactions:** TPPPs engaged in suspicious activity or being used by criminals may have higher than average return rates related to unauthorized transactions. At the merchant level, the criminal merchant may have acceptable return rates compared to the percentage of the TPPP's total transaction volume, but when compared against individual originators, the return rate will be significantly higher.

It is important to understand that credit card transactions, whether conducted through a TPPP or other financial institution, do not have to be significant to be considered suspicious or unusual. For example, there may be a large number of small dollar transactions, repeat customers or donors with no discernible pattern and/or receiving international donations or other payments that do not match with information provided by the customer when they described their business or based on historical activity conducted by the customer. Therefore, it is important to have strong customer and enhanced due diligence and transaction monitoring controls to detect suspicious activity and customers you do not want to do business with.

## MONEY SERVICES BUSINESSES

A money services business (MSB), or money or value transfer service (MVTs) as defined by FATF, transmits or converts currencies. Such businesses usually provide currency exchange, money transmission, check-cashing and money order services.

MSB laws vary by jurisdiction. For example, in the United States, FinCEN defines MSB to include any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities.

- **Dealer in foreign exchange:** These MSBs provide currency exchange services (e.g., USD converted to Euro). They typically operate along international borders, in airports or near communities with high populations of foreign individuals.
- **Check casher:** Check-cashing services may be offered by retail businesses or as a stand-alone operation. Depending on the model, the MSB may cash checks for consumers and/or commercial businesses. In addition to check cashing, these MSBs may also provide other financial services so their customers can pay bills, purchase money orders or transmit funds domestically or internationally.
- **Issuer of traveler's checks or money orders:** The issuer of a money order or traveler's check is responsible for the payment of the item and often uses agents to sell the negotiable items.
- **Money transmitter:** Money transmitters accept currency or funds for the purpose of transferring those funds electronically through a financial agency, institution or electronic funds transfer network. Examples of well-known money transmitters are Western Union, MoneyGram and PayPal.
- **Provider and seller of prepaid access:** Providers of prepaid access arrange for access to funds or to the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number. Sometimes prepaid access can also be referred to as stored value. Prepaid access can be open loop or closed loop.
  - **Open loop prepaid cards** can be used for purchases at any merchant that accepts cards issued for use on the payment network associated with the card and to access cash at any ATM that connects to the affiliated ATM network. Examples of open loop prepaid access usually are branded with the network logo, such as American Express, Visa or MasterCard.
  - **Closed loop prepaid cards** are typically limited to buying goods or services from the merchant issuing the card. Sellers of prepaid access are those who exceed a certain threshold of prepaid access to one individual on a given day.
- **U.S. Postal Service:** Because the U.S. Postal Service sells its own money orders, it is deemed to be an MSB.

FinCEN published a Final Rule in 2012 to expand the MSB definition to detail when an entity qualifies as an MSB based on its activities within the United States, even if none of its agents, agencies, branches or offices are physically located there. The Final Rule arose in part from the recognition that the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations. Absent an exception, MSBs are required to register with FinCEN.

As another example, MSBs in Canada are defined as businesses engaged in foreign exchange dealing, money transferring or cashing or selling money orders, traveler's checks and similar monetary instruments to the public. They are required to register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

An MSB's business model can range from small, independent businesses to large multinational organizations. Organizations can either provide MSB services as their primary business or as an ancillary service to primary retail store operations. Businesses that provide ancillary MSB services typically include grocery stores, drug stores, restaurants and bars. The services provided by these businesses include but are not limited to cashing payroll checks and selling prepaid cards. Although many of these businesses have brick-and-mortar locations, MSBs operating solely on the Internet with no physical presence or a network of agents are increasing.

Traditional MSBs typically provide services to the underserved or unbanked individuals. The focus on this market may put their operations in regions with limited or no banking services. Additionally, they typically provide lower cost services compared to financial institutions for certain service offerings. For example, engaging in domestic or international wire transfers through a financial institution can be time consuming and costly for a consumer. Conducting similar transactions through an MSB can happen quickly and at a much lower cost. Additional services can include bill payments, payday lending and commercial check cashing.

MSBs can be categorized into principals or agents. Principals primarily provide MSB services and act as the issuers of money orders and traveler's checks or the providers of money transmission. In the United States, principal MSBs are required to have written AML policies, procedures and internal controls; appoint a Bank Secrecy Act (BSA) officer; provide education and training, conduct independent reviews and audits and monitor transactions for suspicious activity.

Agents are entities seeking to provide MSB-type services in addition to their existing products and services. An agent may be a principal MSB in that it offers check cashing as its primary service but an agent in that it provides money transmission services through a principal money transmitter MSB. For agents to use such money transmission services, they must enter into an agent service agreement with a principal MSB. An additional byproduct of the principal/agent relationship is that it allows principal MSBs to expand their business and reach a wider customer market without the need for added overhead. As an agent of a principal MSB, the agent is required to follow the same state and federal regulations as a principal MSB (e.g., AML procedures and suspicious activity monitoring).

Examples of how MSBs can be used by criminals follow.

- Fraud in the healthcare industry has grown dramatically in recent years. Healthcare businesses, such as home healthcare businesses, engaged in fraudulent practices will present checks derived from fraud to check cashers who they know will not ask for proof of the payee's identity, will either not file or file false currency transaction reports (CTRs) and not report them to the government for engaging in suspicious activity. The check casher may be compromised by an employee insider or is attempting to be business friendly by avoiding complying with legal or regulatory requirements that are seen as burdens to its customers.
- Criminals obtain low cost workers' compensation insurance policies by grossly deflating payroll amounts. After securing certificates of insurance, organizers rent the certificates to other individuals and businesses for a fee. Because the policies are obtained fraudulently, employees are not covered and are therefore left vulnerable to high-dollar medical costs in the event of an on-the-job injury. The payroll amounts are then concealed by cashing checks at an MSB that circumvents proper bookkeeping measures. The criminal makes a significant amount of money at the detriment of workers.

- Money launderers use money remitters and currency exchanges to make the funds available to the criminal organization at the destination country in the local currency. The launderer/broker then sells the criminal dollars to foreign businessmen wishing to make legitimate purchases of goods for export.

### Case Study

This is an example of money laundering utilizing MSBs from FINTRAC's *Money Laundering Typologies and Trends for Canadian MSBs* report.

Two individuals were suspected of running a mass marketing fraud (MMF) scheme. The perpetrators used MSBs to receive payments from fraud victims in the United States. Counterfeit checks were sent to U.S. residents, who were then instructed to send a portion of these funds back to two individuals perpetrating the fraud.

One of the individuals, who appeared to use two identities and various addresses, was the beneficiary of most of the electronic funds transfers (EFTs) sent through the MSBs. He (or she) regularly received EFTs from U.S.-based fraud victims over a short period of time. Because nearly all of the EFT amounts were below mandatory threshold amounts, it is possible that many more EFTs were sent to the suspected fraud perpetrator before suspicions were triggered regarding the financial activity. Over the course of a year, in excess of three dozen suspicious transaction reports (STRs) were filed on this individual.

The other individual shared the same residential address with the first suspect, although the address was apparently never used when receiving the EFTs. He (or she) was thought to be the mastermind of the scheme, because this individual had been convicted of a large number of fraud-related offenses. The individual had been flagged in reports sent to the government for a series of multiple cash deposits and in relation to depositing MSB-issued checks. The same individual also received Euro-denominated EFTs from Europe.

The main EFT recipient (who used two identities and eight addresses) appeared to be using multiple MSB agents (close to 20 locations) in an attempt to conceal the fraudulent activity. Funds were paid out in checks issued by the MSB. STRs filed by a bank indicate that this individual made a series of deposits into two different bank accounts using cash and checks.

The biggest misconception about the MSB industry is that there is minimal oversight. In fact, many MSBs are overseen by a variety of national and/or local regulators and often maintain compliant AML programs. In addition, they are monitored by the banks that they maintain relationships with. However, the scrutiny to which MSBs are subject can vary greatly, in large part due to the ease with which some MSBs can set up business. Additionally, many MSBs are small (i.e., one-store operators) and may not have robust AML programs compared to their larger, national counterparts. This is why one of the most important aspects of due diligence for a bank when establishing a relationship with an MSB is to confirm that the MSB has implemented a sufficient AML program (e.g., procedures, training and suspicious activity monitoring) and is properly licensed and/or registered in the jurisdictions it operates in.

## INSURANCE COMPANIES

The insurance industry provides risk transfer, saving and investment products to a variety of consumers worldwide, ranging from individuals to large corporations to governments. An important aspect of the way the insurance industry operates is that most of the business conducted by insurance companies is transacted through intermediaries, such as agents or independent brokers. Insurers, with some exceptions, are subject to AML requirements.

The susceptibility of the insurance industry to money laundering is not as high in comparison to other types of financial institutions. For example, policies for property, casualty, title or health insurance typically do not offer investment features, cash build-ups, the option of transferring funds from one to another or other means of hiding or moving money. That said, certain sectors of the insurance industry, such as life insurance and annuities, are a primary target of criminals engaging in money laundering and/or terrorist financing. In a number of ways, the sector's vulnerability to money laundering is similar to that of the securities sector; in some jurisdictions, life insurance policies are even viewed as investment vehicles similar to securities.

According to FATF in its 2004–2005 typologies report, across the whole insurance sector, life insurance appears to be by far the area most attractive to money launderers. Substantial sums can be invested in widely available life insurance products and many feature a high degree of flexibility, whilst at the same time ensuring nonnegligible rates of return. Many life insurance policies are structured to pay a fixed dollar amount upon death of the insured party whereas other life insurance products, such as whole or permanent life insurance, have an investment value, which can create a cash value above the original investment if it is canceled by the policy holder. Such characteristics, whilst of considerable value to the honest policyholder, also offer money launderers various opportunities to legitimize their ill-gotten funds. Furthermore, the most frequently observed individual typology relates to international transactions, which is evidence of the cross-border reach of insurance-related money laundering operations.

For criminals looking to launder funds, life insurance products with no cash surrender value are the least attractive. Those that feature payments of cash surrender value and the opportunity to nominate beneficiaries from the first day of the policy are the most attractive.

Annuities are another type of insurance policy with cash value. An annuity is an investment that provides a defined series of payments in the future in exchange for an up-front sum of money.

Annuity contracts may allow criminals to exchange illicit funds for an immediate or deferred income stream, which usually arrives in the form of monthly payments starting on a specified date. In both cases, a policyholder can place a large sum of money into a policy with the expectation that it will grow based on the underlying investment, which can be fixed or variable. One indicator of possible money laundering is when a potential policyholder is more interested in a policy's cancellation terms than its benefits.

Vulnerabilities in the insurance sector include the following.

- **Lack of oversight/controls over intermediaries:** Insurance brokers have a great deal of control and freedom regarding policies.

- **Decentralized oversight over aspects of the sales force:** Insurance companies may have employees (i.e., captive agents) who are subject to the full control of the insurance company. Noncaptive agents offer an insurance company's products but are not employed by an insurance company. They often work with several insurance companies to find the best mix of products for their clients and may fall between the cracks of multiple insurance companies. Some may work to find the company with the weakest AML oversight if they are complicit with the money launderer.
- **Sales-driven objectives:** The focus of brokers is on selling the insurance products and, thus, they often overlook signs of money laundering, such as a lack of explanation for wealth or unusual methods for paying insurance premiums.

Below are some examples of how money can be laundered through the insurance industry:

- Certain insurance policies operate in the same manner as unit trusts or mutual funds. The customer can overfund the policy and move funds into and out of the policy while paying early withdrawal penalties. When such funds are reimbursed by the insurance company (e.g., by check), the launderer has successfully obscured the link between the crime and the generated funds.
- The purchase and redemption of single premium insurance bonds are key laundering vehicles. The bonds can be purchased from insurance companies and then redeemed prior to their full term at a discount. In such cases, the balance of the bond is paid to a launderer in the form of a sanitized check from the insurance company.
- A free-look period is a feature that allows investors—for a short period of time after the policy is signed and the premium paid—to back out of a policy without penalty. This process allows the money launderer to get an insurance check, which represents cleaned funds. However, as more insurance companies are subject to AML program requirements, this type of money laundering is more readily detected and reported.
- One indicator of possible money laundering is when a potential policyholder is more interested in the cancellation terms of a policy than the benefits of the policy. The launderer buys a policy with illicit money and then tells the insurance company that he has changed his mind and does not need the policy. After paying a penalty, the launderer redeems the policy and receives a clean check from a respected insurer.

The 2004–2005 FATF Money Laundering Typologies report provides some additional typologies related to the insurance industry.

- The funding of insurance policies by third parties (i.e., not the policyholder) who have not been subject to regular identification procedures when the insurance contract was concluded. The source of funds and the relationship between policyholder and third party is unclear to the insurance company.
- The customer actually does not seek insurance coverage but an investment opportunity. Money laundering is enabled by using large sums of money to make substantial payments into life insurance single premium policies, which serve as a wrapped investment policy. A variation on this is the use of large premium deposits used to fund annual premiums. Such policies, which are comparable to single premium policies, again enable the customer to invest substantial

amounts of money with an insurance company. Because the annual premiums are paid from an account that has to be funded with the total amount, an apparently lower money-laundering risk life product will bear the features of the higher risk single premium policy.

In the insurance sector most of the business is conducted through intermediaries. As a result, on most occasions it is intermediaries' application of the AML regulatory requirements that is unsatisfactory.

When a company assesses laundering and terrorist financing risks, it must consider whether it permits customers to

- use cash or cash equivalents to purchase insurance products;
- purchase an insurance product with a single premium or lump-sum payment; and
- borrow money against an insurance product's value.

## SECURITIES BROKER-DEALERS

The securities industry provides opportunities for criminals to engage in money laundering and terrorist financing anonymously, given the varying levels of AML program requirements in different types of businesses and the high volume of transactions. The world capital markets are vast in size, dwarfing deposit banking. According to the World Bank, in 2015 the market capitalization of listed companies alone totaled over \$61.7 trillion.

FATF has urged money laundering controls for the securities field since 1992, in conjunction with the Montreal-based International Organization of Securities Commissions (IOSCO), a global association of governmental bodies that includes the Commodity Futures Trading Commission (CFTC), which regulates the securities and futures markets. The difficulty in dealing with laundering in the securities field is that, usually, little currency is involved. It is an industry that runs by electronic transfers and paper. Its use in the money laundering process is generally after launderers have placed their cash in the financial system through other methods.

Aspects of the industry that increase its exposure to laundering are

- its international nature;
- the speed of the transactions;
- the ease of conversion of holdings to cash without significant loss of principal;
- the routine use of wire transfers to, from and through multiple jurisdictions;
- the competitive, commission-driven environment, which, like private banking, provides ample incentive to disregard the source of client funds;
- the practice of brokerage firms of maintaining securities accounts as nominees or trustees, thus permitting concealment of the identities of the true beneficiaries; and
- weak AML programs that do not have effective customer due diligence (CDD), suspicious activity monitoring or other controls.

The illicit money laundered through the securities sector can be generated by illegal activities both from outside and from within the sector. For illegal funds originating outside the sector, securities transactions for the creation of legal entities may be used to conceal or obscure the source of these funds (i.e., layering). In the case of illegal activities within the securities market itself—for example, embezzlement, insider trading, securities fraud and market manipulation—the transactions or manipulations generate illegal funds that must then be laundered. In both cases, the securities sector offers launderers the potential for a double advantage: allowing them to launder illegal funds and to acquire additional profit.

Money laundering can occur in the securities industry in customer accounts that are used only to hold funds and not for trading. This allows launderers to avoid banking channels where the launderer may believe there are more stringent money laundering controls. Other indications of money laundering are wash trading or offsetting transactions. This involves the entry of matching buys and sells in particular securities, which creates the illusion of trading. Wash trading through multiple accounts generates offsetting profits and losses and transfers of positions between accounts that do not appear to be commonly controlled.

The 2009 FATF *Money Laundering and Terrorist Financing in the Securities Sector* typologies report identified the following areas as presenting the greatest money laundering vulnerabilities.

- Wholesale markets
- Unregulated funds
- Wealth management
- Investment funds
- Bearer securities
- Bills of exchange

Several challenges that are unique to the securities sector include the following.

- **Variety and complexity of securities**

Security offerings are broad with some products tailored to the needs of a single customer whereas others are designed for sale to the general public. Products range from the simple and almost universally known to the relatively complex and esoteric. Some knowledge of the underlying security is typically required in addressing risk.

- **High-risk securities**

While most securities are issued by legitimate companies, there are risks posed by securities that are underregulated or established for illegitimate purposes. In the United States, securities that are not traded on regulated exchanges are typically sold over-the-counter, with tiers such as pink sheets that require only minimal reporting, thus making it easy to obscure information such as beneficial owners. This can make it difficult to determine associations with sanctioned jurisdictions or companies. Securities firms are required to not only identify securities that may cause risks but also develop processes to restrict trading of those securities, often on dozens of platforms.

- **Multiple layers and third-party risk**

The securities industry has many participants, including financial institutions and broker-dealers, financial advisors, transfer agents, securities lenders, custodians, introducing brokers and sales agents. The many layers of intermediaries, who may also cross borders, make standardizing controls difficult and further challenge overall compliance.

FATF has identified a number of suspicious indicators within the global securities markets. Those particularly relevant to the securities sector include

- a customer with a significant history with the securities firm who abruptly liquidates all of his or her assets in order to remove wealth from the jurisdiction;
- a customer who opens an account or purchases a product without regard to loss, commissions or other costs associated with that account or product, including with early cancellations of long-term securities;
- the securities account is used for payments or outgoing wires with little or no securities activities (e.g., account appears to be used as a depository account or a conduit for transfers);
- a customer's transactions include a pattern of sustained losses, which may be indicative of transferring value from one party to another;
- transactions where one party purchases securities at a high price and then sells them at a considerable loss to another party, which may be indicative of transferring value from one party to another;
- a customer who is unfamiliar with a financial product's performance and specifications but wants to invest in it nonetheless;
- a customer who is known to have friends or family who work for the securities issuer or a trading pattern suggests that he or she may have nonpublic information;
- two or more unrelated accounts at a securities firm trade an illiquid or low-priced security (penny stock) suddenly and simultaneously; and
- a customer who deposits physical securities that (1) are in large quantities, (2) are titled differently from the name of the account, (3) do not bear a restrictive legend even though the history suggests that they should or (4) that lack sense in the method by which they were acquired.

Case Study

In June 2016, Albert Fried & Co. (AFCO), a U.S.-registered broker-dealer, settled charges with the SEC for failing to monitor a customer's trades for suspicious activity as required under federal securities laws. Customer A deposited with and sold through AFCO more than 119 million shares of four penny stocks over a 4-month period. On one day, the customer's trades represented over 85 percent of the daily volume in a single stock and on numerous other days the trading accounted for over 50 percent.

Numerous red flags should have raised concerns for AFCO and prompted further investigation or reporting, such as (1) the stock issuers were the subject of promotional campaigns at the time of the customer's trading, (2) the broker-dealer was aware that the issuer underwent a 5:1

reverse stock split shortly after Customer A deposited that issuer's securities into its AFCO account, (3) the broker-dealer received numerous regulatory and criminal inquiries regarding Customer A's trading in at least three securities and (4) the Commission suspended trading in an issuer's stock only 3 months after Customer A sold large volumes of the issuer's securities.

Broker-dealers have a duty to detect red flags and perform additional due diligence, especially when the indicators are related to penny stock transactions. The use of broker-dealers by criminals to launder proceeds of crime or conduct fraud is common throughout the industry. Canada's FINTRAC provides a good case study of such a scheme.

### Case Study

A group of individuals were suspected of manipulating the share price of Company X, which traded over-the-counter in the United States, in what is commonly referred to as a "pump and dump" scheme. Individual 1 purchased shares in the company at a low price. Typical of the "pump" aspect of these types of schemes, the group produced fraudulent reports on the company's prospects that caused the shares to increase sharply in value. According to law enforcement, the perpetrators of the scheme approached an organized crime group to launder the criminal proceeds that resulted from the sale of shares following the artificial price inflation.

Individual 2 deposited physical share certificates of Company X into a brokerage account. Individual 2 was suspected of being a nominee for the organized crime group. Shortly after the deposits of the physical share certificates, Individual 2 engaged in what appeared to be a structured sale of the shares, characteristic of the "dump" phase of this type of fraud. Following the sale of the shares, Individual 2 requested early settlement in the form of certified checks.

The certified checks were deposited into Individual 2's bank account held at a financial institution that was not affiliated with the brokerage firm. Individual 2 ordered multiple EFTs to a company located in Central America, the beneficial owner of which was Individual 1.

Retail broker-dealers are the industry's frontline defense—and its most vulnerable access point. They are under constant management pressure to expand their client base and to manage more assets. The more assets in a client's account, the more commission will be generated. A money launderer can potentially use this to his advantage by promising a large or steady commission stream. As such, it is important for broker-dealers to understand who they are doing business with and to monitor for suspicious activity.

In the United States, the SEC and the Financial Industry Regulatory Authority (FINRA), as directed by the Bank Secrecy Act (BSA) regulatory rules, have implemented requirements for broker-dealers at both small and large firms to implement AML programs that include an appointed BSA Officer, performing CDD, suspicious activity monitoring, training and an independent audit. These requirements also subject broker-dealers to oversight by either the SEC or FINRA (or both) to monitor if and how they are complying with the AML program requirements. Lack of, or weak, AML program requirements can lead to substantial monetary and criminal penalties.

## Nonfinancial Businesses and Professions

---

### CASINOS

Casinos are among the most proficient cash-generating businesses. High rollers, big profits, credit facilities and a variety of other factors combine to create a glittering amount of cash that flows from the house to the players and back. Where it is legally permitted, billions of dollars readily flow between customer and casino.

Casinos and other businesses associated with gambling, such as bookmaking, lotteries and horse racing, continue to be associated with money laundering because they provide a ready-made excuse for recently acquired wealth with no apparent legitimate source. The services offered by casinos will vary depending on the jurisdiction in which they are located and the measures taken in that jurisdiction to control money laundering.

Money laundering through casinos generally occurs in the placement and layering stage (e.g., converting the funds to be laundered from cash to checks and utilizing casino credit to add a layer of transactions before the funds are ultimately transferred out). A launderer can buy chips with cash generated from a crime and then request repayment by a check drawn on the casino's account. Often, rather than requesting repayment by check in the casino where the chips were purchased with cash, the gambler says that he will be traveling to another country in which the casino chain has an establishment, asks for his credit to be made available there and withdraws it in the form of a check in the other jurisdiction. Money launderers can also establish a casino line of credit and use illegitimately obtained funds as a repayment on the credit line.

In its 1997–1998 typologies report, FATF reported that gaming businesses and lotteries were being used increasingly by launderers. FATF gave examples of gambling transactions that enabled drug dealers to launder their money through casinos and other gambling establishments. One laundering technique connected with horse racing and gaming is when the person will actually gamble the money to be laundered but in such a way as to be reasonably sure of ultimately recovering his or her stake in the form of checks issued or funds transfers by the gambling or betting agency and reflecting verifiable winnings from gaming. This method makes it more difficult to prove the money laundering because the person has actually received proceeds from gambling.

Junkets, a form of casino-based tourism, also present significant money laundering risk because junket participants largely rely on third parties, junket operators, to move the funds across borders and through multiple casinos, creating layers of obscurity around the source of funds and ownership of the money and the identities of the players. In some jurisdictions, casinos may enter into a contractual agreement with a junket operator to rent a private gaming room, and in some situations it is the junket operator, not the casino, that monitors player activity and issues and collects credit. Additionally, some jurisdictions allow junket operators to pool funds, which obscures the spending of individual customers. In certain regions, licensed junket operators act as fronts for junket operators in another country. The front operators supply players to a casino through a casino's licensed junket companies, which may not qualify for a license in the country where the players will be

gambling. Such unlicensed subjunket operators can act as unlicensed collectors of credit and may have ties to organized crime networks. This poses serious risk and can lead a casino to engage in informal arrangements with junket operators that are inconsistent with AML/CFT policies.

In its 2009 Report, FATF recognized that a number of jurisdictions do not require licensing of junket operators and their agents, further increasing the risks described above, and stressed the need to ensure that junket operators are not under criminal influence and to ensure that financial transactions are transparent and subject to relevant AML/CFT measures.

FinCEN's 2008 Guidance and FATF's 2009 *Vulnerabilities of Casinos and Gaming Sector* report identified specific behaviors to watch for.

- Attempts to evade AML reporting or record-keeping requirements, such as
  - a customer pays off a large credit debt, such as markers or bad checks, over a short period of time through a series of currency transactions, none of which exceeds the reportable threshold;
  - two or more customers each purchase chips in small amounts, engage in minimal gaming, then combine the funds to request a casino check for the chips presented;
  - a customer receives a large payout in excess of \$10,000 but requests currency of less than \$10,000 and the balance paid in chips. He then goes to the cage and redeems the remaining chips in the amounts less than the reporting threshold;
  - a customer structures the transaction, by often involving another customer, to avoid filing of the CTR or another tax form; and
  - a customer reduces the amount of chips presented for a cash-out when asked for ID to stay under the reportable threshold.
- Using the cage solely for its banking-like financial services, such as
  - a customer wires funds derived from nongaming proceeds, to or through a bank or nonbank financial institution located in a country that is not his residence or place of business; and
  - a customer appears to use a casino as a temporary repository for funds by making frequent deposits into the casino account and, within a short period of time, requesting money transfers to a domestic or foreign-based bank account.
- Minimal gaming activity without a reasonable explanation, such as
  - a customer purchases a large amount of chips, engages in minimal gaming and then redeems the chips for a casino check;
  - a customer uses an established casino credit line to purchase chips, engages in minimal play, then pays off the credit in currency and redeems the chips for a casino check;
  - a customer makes a large deposit using small denomination bills and withdraws it in chips at the table; engages in minimal play, then exchanges the chips at the cage for large denomination bills;

- a customer inserts large amounts of small-denomination bills into a slot machine (“bill-stuffing”), engages in minimal or no play and exchanges the voucher at the kiosk or cage for large-denomination bills or requests a casino check for what appears to be a legitimate winning credit from a slot machine;
  - a customer frequently purchases chips with currency under a reportable threshold, engages in minimal play and walks away without cashing out the chips; and
  - a customer transfers funds to a casino for deposit into a front money account, withdraws it in chips at the table and engages in minimal play, then requests the chips to be exchanged for a casino check.
- Unusual gaming and transaction patterns, such as
    - two customers frequently bet large amounts to cover between them both sides of an even bet, such as
      - > betting both “red and black” or “odd and even” on roulette,
      - > betting both “with and against” the bank in baccarat and
      - > betting the “pass line” or “come line” and the “don’t pass line” and “don’t come line” in craps;
    - a customer routinely bets both sides of the same line for sporting events (i.e., betting both teams to win), and thus the amount of overall loss to the customer is minimal (known as hedging);
    - a customer requests the issuance of a casino check payable to third parties, or without a specified payee;
    - a customer makes large deposits or pays off large markers with multiple instruments (cashier’s checks, money orders, traveler’s checks or foreign drafts) in amounts of less than \$3,000 indicating an attempt to avoid identification requirements;
    - a customer withdraws a large amount of funds from a deposit account and requests multiple casino checks to be issued, each less than \$10,000; and
    - a customer establishes a high value deposit that remains dormant for an extended period of time, then withdraws or transfers the funds.

The risk of money laundering comes not only from the specific behaviors but also the type of customer casinos choose to conduct business with. Players often build a reputation of a high roller as long as they show big play, without being subject to the due diligence necessary to determine the source of funds. The biggest mistake a casino can make is to allow play and accept the revenue without reasonably determining the source of gaming funds. U.S. casinos may soon have to vet where their high rollers’ funds come from under a requirement being developed by the U.S. Treasury Department. Although the existing rules do not explicitly require the source of funds to be known, it is recommended that casinos require more information from certain customers to shed light on high-risk transactions, such as international wire transfers and large cash deposits, as part of the risk-based approach.

The United States, through FinCEN, has been one of the most aggressive authorities on issuing anti-money laundering program deficiency penalties to some of the largest casinos in the industry.

- **Tinian Dynasty Hotel & Casino fined \$75M (2015):** Casino failed to develop and implement an AML program (no dedicated AML officer, failure to develop and implement AML policies and procedures, no independent tests of the AML program), which led the casino to fail to file thousands of CTRs and have employees assist wealthy VIP patrons engage in suspicious transactions (especially structuring).
- **Trump Taj Mahal fined \$10M (2015):** Casino failed to maintain an effective AML program, failed to file SARs and CTRs and failed to maintain appropriate records.
- **Caesar's Palace fined \$9.5M (2015):** Casino "allowed some of the most lucrative and riskiest financial transactions to go unreported," promoted private salons in the United States and abroad without appropriately monitoring transactions, such as wire transfers, for suspicious activity and openly allowed patrons to gamble anonymously.
- **Sparks Nugget fined \$1M (2016):** Casino "had a systemic breakdown in its compliance program" and disregarded its compliance manager. Rather than file rightfully prepared suspicious activity reports (SARs), Sparks Nugget instructed the compliance manager to avoid interacting with regulatory auditors and prevented her from reviewing a copy of the completed regulatory exam report.

In addition to ensuring adequate record-keeping and reporting requirements, casino AML/CFT programs should establish a process that will enable the casino to reasonably determine sources of funds and allow customer due diligence to be conducted at the time the funds are accepted, often with a customer already on property and ready to game, rather than relying exclusively on the after-the-fact back-of-house compliance investigation.

Although the notion of on-demand enhanced know your customer (KYC) and source of fund questioning is relatively new to casinos, there are many ready-to-use tools developed specifically for the industry's front-of-house operations. The best processes will combine information from various international sources—criminal and judicial, securities and exchanges, financial, government and worldwide lists, political exposure, negative news, business associations—and ID verification, making the due diligence possible directly from the frontline of operations.

#### *Case Study*

In 2013, The U.S. Department of Justice concluded its money laundering investigation into Las Vegas Sands Corp., resulting in a \$47 million settlement to avoid criminal prosecution in connection with funds gambled by high rollers in Las Vegas, particularly by Zhenli Ye Gon, a Chinese-Mexican businessmen who owned a pharmaceutical factory in Mexico.

Between 2006 and 2007, Ye Gon deposited over \$50 million at the Sands, principally via wire transfers and cashier's checks, which was allegedly proceeds of crime tied to the illegal manufacture of synthetic drugs, and received as much as \$100M. In 2007, \$207 million cash was seized from Ye Gon's residence in Mexico, the largest-ever seizure of cash.

According to the evidence gathered by the DOJ, Ye Gon took steps to actively avoid detection of money laundering and used classic money laundering methods. Ye Gon and his associates wired money to the Sands and its subsidiary companies from two different banks and seven different Mexican money exchange houses known as casa de cambios. The wire originators included several companies and individuals the Sands could not link to Ye Gon to. According to the DOJ, Ye Gon also transferred funds from Mexican casas de cambios to Sands' subsidiary in Hong Kong for subsequent transfers to Las Vegas. In many instances, Ye Gon's wire transfers lacked sufficient information to identify him as the intended beneficiary. Additionally, Sands allowed Ye Gon to conduct several transfers of funds to an account that did not identify its association with the casino, specifically an aviation services account of Interface Employee Leasing, used to pay pilots operating the company's aircraft.

Casinos are not limited to physical locations. In fact, online casinos and gaming operations have increased their presence in recent years. Online gaming may be regulated in certain jurisdictions; however, a lot of online gaming companies operate illegally. For example, in the United Kingdom, the Gambling Commission requires a license for remote gambling where the business operates in the UK and any part of its gambling equipment is located in the UK or if the equipment is located outside the UK but the business operates through a British-facing business. Online gaming is also regulated in Antigua and Barbuda under the Interactive Gaming and Interactive Wagering Regulations and required to establish compliance programs.

Nevertheless, online gambling provides an excellent method of money laundering for cyber criminals because transactions are conducted principally through credit or debit cards. Site operators are typically unregulated offshore firms. This can affect a financial institution because the Internet gambling sites often have accounts in offshore banks that, in turn, use reputable domestic correspondent banks. Tracing the source and ownership of illegal money that moves through these accounts can be difficult for enforcement and regulatory agencies.

Due to the inconsistent regulatory environment and susceptibility to cyber criminals, some credit card issuers no longer allow the use of their credit cards for online gambling. Financial institutions screen merchant codes that identify the type of business accepting the credit card and transaction codes for card not present (i.e., the cardholder is not physically in the casino to process the transaction via a card reader). The bank can thus block Internet gambling transactions. However, online gambling can be funded in numerous ways beyond credit cards, such as prepaid cards, wire transfers, peer-to-peer transfer, virtual currency and mobile phone carrier billing.

MONEYVAL is the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. In its April 2013 research report entitled, *The Use Of Online Gambling For Money Laundering And The Financing Of Terrorism Purposes*, MONEYVAL identified numerous potential typologies for money laundering. Some examples include the following.

- A money launderer colludes with an operator of an offshore online gambling operation and deposits funds obtained from criminal activities into the gambling account and withdraws such funds as winnings. The website operator keeps a percentage of the proceeds as a commission while the launderer declares the winnings to the tax authorities and then uses the funds for legitimate purposes.

- A money launderer colludes with professional gamblers to place illegally obtained funds on online gambling websites. The gamblers keep a commission from any winnings made before transferring the remaining funds to the launderer.
- A money launderer deposits funds into an online gambling account by using a stolen identity. He or she bets using the funds and receives payouts for the winnings or sustains acceptable losses.

## DEALERS IN HIGH-VALUE ITEMS (PRECIOUS METALS, JEWELRY, ART ETC.)

The European Directive on money laundering provides a common framework for including trade in gold, diamonds and other high-value items within anti-money laundering monitoring systems. Effective January 2006, the USA PATRIOT Act required certain dealers in covered and finished goods, including precious metals, stones and jewels, to establish an anti-money laundering program. However, in many other jurisdictions these industries are yet to be regulated for money laundering control purposes.

In July 2015, FATF released a report titled, *Money Laundering/Terrorist Financing Risks and Vulnerabilities Associated With Gold*, which reinforced prior typology reports. Gold has high intrinsic value in a relatively compact and easy to transport form. It can be bought and sold easily and often with anonymity for currency in most areas of the world. It is more readily accepted than precious stones, especially because it can be melted down into many different forms. It holds its value regardless of the form it takes—whether as bullion or as a finished piece of jewelry—and is thus often sought after as a way of facilitating the transfer of wealth. For some societies, gold carries an important cultural or religious significance that adds to its demand.

Here are two of the key findings from the report.

- 1) Gold is an extremely attractive vehicle for laundering money. It provides a way for criminals to convert their illicit cash into anonymous, transferable assets.
- 2) The gold market is a target for criminal activity because it is lucrative. Understanding and knowing the various stages of the gold market and types of predicate offenses is critical in identifying money laundering.

### Case Study

In Operation Meltdown, U.S. Homeland Security Investigations (HSI) investigators uncovered a carousel scheme in which jewelers were converting the proceeds from drug sales into the equivalent value in gold. The scheme involved a criminal organization with links to gold suppliers in the New York area that were laundering millions of dollars in drug proceeds. The HSI investigation disclosed that the exported gold from Colombia was described as “gold pigments” and upon importation into the United States the same merchandise was then described as “gold bullion.” The gold bullion was then transported to New York, where jewelers who were cooperating with drug trafficking organizations disguised the gold in a wide range of common objects, such as wrenches, nuts, bolts, belt buckles and trailer hitches. These items were exported back to Colombia at a declared value far below the worth of their weight in gold. Upon arrival in Colombia, the same gold was recast into bullion and exported again to the United States as “gold

pigment.” The investigation of this case resulted in the arrest of 23 jewelers charged with money laundering and others, along with the seizure of 140 kg of gold, more than 100 loose diamonds, \$2.8 million, 118 kg of cocaine, six guns and two vehicles.

In certain instances, some of the transactions in a particular scheme do not take place at all but are represented with false invoicing. The paperwork is then used to justify transferring funds to pay for the shipments. The false invoicing scheme, whether overbilling or underbilling for the reputed goods or services provided, is a common money laundering technique.

The following transactions are also vulnerable and require additional attention.

- **Payments or returns to persons other than the owner:** If one person delivers precious metal for refining and asserts ownership of the metal and authority to sell it but directs payments to be made to another person, that transaction may be questionable. The “dealer in precious metal” is being used to transfer an asset not only from one form into another—unrefined gold to refined gold or money within the international finance system—but also from one person to another.
- **Precious metal pool accounts:** These accounts are maintained by a small number of large and sophisticated precious metal companies and have worldwide scope. They receive and hold precious metal credits for a customer, which can be drawn on by that customer. The customer can request the return of the precious metals, the sale and return of monetary proceeds or the delivery of precious metal to another person. Thus, a refining customer in one country can deliver gold scrap for refining, establish a gold credit in the refiner’s pool account system and subsequently have delivery made by the refiner to another person, based upon that credit.

### Case Study

On June 5, 2003, U.S. Immigration and Customs Enforcement (ICE) agents arrested 11 individuals at seven jewelry stores in Manhattan’s diamond district on charges of participating in an international money laundering scheme. The agents had received information that Colombian drug cartels were laundering money through the purchase, smuggling and resale of diamonds and gold. The cartels were instructing their U.S. employees to buy precious stones in New York with drug proceeds and then to smuggle them to Colombia, where they were resold to refiners for clean pesos that the traffickers could use risk-free. Based on this information, ICE agents launched an investigation in 1999 into several New York jewelers alleged to be involved in the money laundering. According to the charges, the jewelers were approached by undercover agents posing as drug dealers. The agents told the jewelers they were looking to buy gold and diamonds with illicit funds so they could smuggle these precious metals to Colombia and then resell them to refiners for clean cash. According to the charges, the jewelers willingly accepted \$1 million in drug funds from the undercover agents. The jewelers offered to smelt the gold into small objects, such as belt buckles, screws and wrenches, to facilitate smuggling the transfer into Colombia.

Illegal trade in diamonds has become an important factor in armed conflict in certain areas of the world, and terrorist groups may be using diamonds from these regions to finance their activities.

Individuals and entities in the diamond sector have also been involved in complex diamond-related money laundering cases. As with gold, the simplest typology involving diamonds consists of the direct purchase of the gems with ill-gotten money.

With regard to dealers in high-value items, FATF says that the more common types of laundering activity include retail foreign exchange transactions, forged or fraudulent invoicing, commingling of legitimate and illicit proceeds in the accounts of diamond trading companies and, in particular, international fund transfers among these accounts. Some of the detected schemes were covers for laundering the proceeds of illicit diamond trafficking. In others, diamond trading was used as a method for laundering proceeds generated by other criminal activity.

The multi-million-dollar fine art industry can also serve as a convenient money laundering vehicle. Anonymous agents at art auction houses bid millions of dollars for priceless works. Payment is later wired to the auction house by the agents' principals from accounts in offshore havens. It is an ideal mechanism for the money launderer.

### Case Study

Operation Dinero was a famous 1992 joint DEA and IRS operation in which the agencies set up a fake bank in Anguilla targeting the financial networks of international drug traffickers. Several undercover companies were established by law enforcement in different jurisdictions as fronts designed to supply laundering services to the traffickers. Members of the Cali cartel engaged in transactions with the "bank" to sell three masterpieces by Picasso, Rubens and Reynolds that had a combined value of \$15 million. The works were later seized by the United States.

Art and antiques dealers and auctioneers should follow these tips to lessen their money laundering risks.

- Require all art vendors to provide names and addresses. Ask that they sign and date a form that states that the item was not stolen and that they are authorized to sell it.
- Verify the identities and addresses of new vendors and customers. Be suspicious of any item whose asking price is not commensurate with its market value.
- If there is reason to believe an item might be stolen, immediately contact the Art Loss Register ([www.artloss.com](http://www.artloss.com)), the world's largest private database of stolen art. The database contains more than 100,000 items reported by enforcement agencies, insurers and individuals as being stolen.
- Look critically when a customer asks to pay in cash. Avoid accepting cash payments unless there is a strong and reputable reason.
- Be aware of money laundering regulations.
- Appoint a senior staff member to whom employees can report suspicious activities.

## **TRAVEL AGENCIES**

Travel agencies can also be used as a means for money launderers to mix illegal funds with clean money to make the illegal funds look legitimate, by providing a reason to purchase high-priced airline tickets, hotels and other vacation-related expenses.

### Case Study

Operation Chimborazo, named for the famous Ecuadorean mountain, was a large multinational effort in the mid-1990s aimed at businesses suspected of laundering drug proceeds. The operation focused on the money laundering organization of Hugo Cuevas Gamboa, a reputed principal launderer for the Cali Cartel. In 1994, law enforcement teams cracked down on several businesses in Latin American countries, which included travel agencies. During a raid in Argentina, the authorities arrested the owners of a travel agency that was part of an organization that laundered \$50 million per week in drug proceeds from 22 countries.

Money laundering can occur in travel agencies in the following manner.

- Purchasing an expensive airline ticket for another person who then asks for a refund.
- Structuring wire transfers in small amounts to avoid record-keeping requirements, especially when the wires are from foreign countries.
- Establish tour operator networks with false bookings and documentation to justify significant payments from foreign travel groups.

## **VEHICLE SELLERS**

This industry includes sellers and brokers of new vehicles, such as automobiles, trucks and motorcycles; new aircraft, including fixed-wing airplanes and helicopters; new boats and ships; and used vehicles.

Laundering risks and ways laundering can occur through vehicle sellers include

- structuring cash deposits below the reporting threshold or purchasing vehicles with sequentially numbered checks or money orders;
- trading in vehicles and conducting successive transactions of buying and selling new and used vehicles to produce complex layers of transactions; and
- accepting third-party payments, particularly from jurisdictions with ineffective money laundering controls.

Most money laundering cases dealing with vehicle dealers have one common element: the unreported use of currency to pay for the automobiles.

There have also been cases where authorities have charged that a car dealer laundered money by allowing a drug dealer to trade in his cars for cheaper models and to be paid in checks, not cash, for the difference. In one such down-trading money laundering scheme, a drug dealer traded in his \$37,000 Porsche for a \$17,000 Ford Bronco and the car dealer allowed the down-trade, knowing that the customer was a drug dealer, in violation of the anti-money laundering law.

### Case Study

In 2011, The U.S. Department of the Treasury identified the Lebanese Canadian Bank SAL together with its subsidiaries (LCB) as a financial institution of primary money laundering concern for the bank's role in facilitating the money laundering activities of an international narcotics trafficking and money laundering network. The U.S. authorities determined that LCB—through

management complicity, failure of internal controls and lack of application of prudent banking standards—had been used extensively by persons associated with international drug trafficking and money laundering networks.

In this network, a U.S. designee, Ayman Joumaa, coordinated the transportation, distribution and sale of multiton bulk shipments of cocaine from South America and laundered the proceeds—as much as \$200 million per month—from the sale of cocaine in Europe and the Middle East. The proceeds were laundered through various methods, including through car dealerships. Specifically, Ayman Joumaa deposited bulk cash into multiple exchange houses, including the one that he owned, which then deposited the currency into their LCB accounts. He or the exchange houses then instructed LCB to perform wire transfers to move some of the funds through LCB's U.S. correspondent accounts via suspiciously structured electronic wire transfers to multiple U.S.-based used car dealerships—some of which were operated by individuals who have been separately identified in drug-related investigations. The recipients used the funds to purchase vehicles in the United States, which were then shipped to West Africa and/or other overseas destinations, with the proceeds ultimately repatriated back to Lebanon.

## **GATEKEEPERS: NOTARIES, ACCOUNTANTS, AUDITORS AND LAWYERS**

Countries around the world have been putting responsibilities on professionals, such as lawyers, accountants, company formation agents, auditors and other financial intermediaries, who have the ability to either block or facilitate the entry of illegitimate money into the financial system.

The responsibilities of such gatekeepers include requiring them to identify clients, to conduct due diligence on their clients, to maintain records about their clients and to report suspicious client activities. Some of these rules also prohibit gatekeepers from informing or tipping off clients who are the subject of the suspicious transaction reports. Violations may subject gatekeepers to prosecution, fines and even imprisonment.

In the European Union and several other countries, mandatory anti-money laundering duties already apply to gatekeepers. FATF's 40 Recommendations also cover independent legal professionals (*see Chapter 3 for more on the Recommendations*), including lawyers and legal professionals and other gatekeepers.

In its 2013 typology report, FATF stated that the following functions provided by lawyers, notaries, accountants and other professionals are the most useful to a potential money launderer.

- Creating and managing corporate vehicles or other complex legal arrangements, such as trusts: Such arrangements may serve to obscure the links between the proceeds of a crime and the perpetrator.
- Buying or selling property: Property transfers serve as either the cover for transfers of illegal funds (layering stage) or the final investment of proceeds after they pass through the initial laundering process (integration stage).
- Performing financial transactions: Sometimes these professionals may carry out various financial operations on behalf of the client (for example, issuing and cashing checks, making deposits, withdrawing funds from accounts, engaging in retail foreign exchange operations, buying and selling stock and sending and receiving international funds transfers).

- Providing financial and tax advice: Criminals with large amounts of money to invest may pose as individuals hoping to minimize tax liabilities or seeking to place assets out of reach in order to avoid future liabilities.
- Providing introductions to financial institutions.
- Undertaking certain litigation.
- Setting up and managing a charity.

In many cases, criminals will use legal professionals to provide an impression of respectability in order to dissuade questioning or suspicion from financial institutions and to create an added step in the chain of any possible investigations. Additionally, legal professionals may deliberately misuse a client's legitimate accounts to conduct transactions without the client's knowledge.

The report also describes red flag indicators of money laundering of terrorism financing.

1. The client

- a. is overly secretive;
- b. is using an agent or an intermediary or avoids personal contact without a good reason;
- c. is reluctant to provide or refuses to provide information or documents usually required to enable the transaction's execution;
- d. holds or has previously held a senior public position or has professional or family ties to such individuals;
- e. is known to have been the subject of investigation for an acquisitive crime (i.e., one where the offender derives material gain from the crime, such as theft or embezzlement);
- f. is known to have ties to criminals; and/or
- g. shows unusual interest and asks repeated questions on the procedures for applying ordinary standards.

2. The parties

- a. are native to, residents in or incorporated in a high-risk country;
- b. are connected without an apparent business reason;
- c. are tied in a way that generates doubts as to the real nature of the transaction;
- d. appear in multiple transactions over a short period of time;
- e. are incapacitated or under legal age and there is no logical explanation of their involvement;
- f. attempt to disguise the real owner or parties to the transaction;
- g. are not directing the transaction—rather, the person directing the operation is not one of the formal parties to the transaction; and/or
- h. do not appear to be suitable representatives.

3. The source of funds
  - a. is provided using unusual payment arrangements;
  - b. is collateral located in a high-risk country;
  - c. represents a significant increase in capital for a recently incorporated company, including foreign capital, without a logical explanation;
  - d. represents unusually high capital in comparison with similar businesses;
  - e. stems from a security transferred with an excessively high or low price attached; and/or
  - f. stems from large financial transactions that cannot be justified by the corporate purpose.
4. The lawyer
  - a. is at a significant distance from the client or transaction without a legitimate or economic reason;
  - b. does not have experience in providing the particular services needed;
  - c. is being paid substantially higher than usual fees without a legitimate reason;
  - d. is frequently changed by the client, or the client has multiple legal advisors without legitimate reason; and/or
  - e. is providing services previously refused by another professional.
5. The retainer involves
  - a. transactions that are unusual with regards to the type of operation and the transaction's typical size, frequency or execution;
  - b. transactions that do not correspond to the client's normal business activities and show that he does not have a suitable knowledge of the nature, object or the purpose of the professional performance requested;
  - c. the creation of complicated ownership structures or structures with involvement of multiple countries when there is no legitimate or economic reason;
  - d. a client transaction history that does not have documentation to support company activities;
  - e. inconsistencies and unexplained last minute changes to instructions;
  - f. no sensible commercial, financial or tax reason for the transactions or increased complexity that unnecessarily results in higher taxes or fees;
  - g. exclusively keeping documents or other goods, holding large deposits or otherwise using the client account without provision of legal services;
  - h. abandoned transactions without concern for fee level or after the receipt of funds;
  - i. a power of attorney sought for the administration or disposal of assets under unusual circumstances without logical reason;

- j. litigation that is settled too easily or quickly with little or no involvement of legal professional retained; and/or
- k. requests for payments to third parties without substantiating reason or corresponding transaction.

FATF cites the following example in its typologies report of how a lawyer may help set up a complex laundering scheme.

#### Case Study

An Eastern European was acting under an alias as the director of a company for which he opened an account with a Belgian bank. Transfers were made to this account from abroad, including some on the instructions of “one of our clients.” The funds were then used to issue a check to a notary for the purchase of a property. The notary was drawn to the fact that some time after the purchase, the company went into voluntary liquidation, and the person concerned bought the property back from his company for an amount considerably above the original price. In this way the individual was able to insert money into the financial system for an amount corresponding to the initial sale price plus the capital gain. He was thus able to use a business account, front company customer, purchase of real estate, cross-border transaction and wire transfers to launder money that, according to police sources, came from activities related to organized crime. It appeared that the company acted as a front set up merely for the purpose of carrying out the property transaction.

#### Case Study

An attorney was convicted by a jury of conspiracy to commit money laundering. The attorney helped to invest the drug proceeds of his client by forming a corporation in the name of the client's wife and arranging a loan from the corporation to another (noncriminal) client. He then drafted a phony construction work contract, making the repayment of the loan appear to be payment for construction work performed by the company. He also drew up a promissory note, which the wife signed, but did not provide copies of the note to either party. The attorney also advised his client how to deposit the cash from the loan without triggering reporting requirements. The appeals court upheld the attorney's conviction but remanded him for resentencing after finding that the district court abused its discretion by not applying a sentencing enhancement based on the attorney's use of special skills (legal skills) in committing the offenses of conviction.

The issue of requiring attorneys to be gatekeepers in the AML/CFT area has been controversial due to the fact that attorneys have confidential relationships with their clients. Various alternatives have been discussed and debated, including

- deferring regulation until adequate education is conducted;
- imposing internal controls and due diligence duties on lawyers with regard to non-privileged communications;
- using a joint government-private sector body to regulate lawyers who engage in financial activities, requiring registration with and regulation by an agency; and
- devising a new hybrid approach, such as through guidance notes or best practices standards from FATF.

Gatekeeper issues in the United States are focused on the scope of the requirements, particularly the definition of the financial transactions to which reporting requirements would apply. Many regulators within the United States want the scope to coincide with the European Union Directive, which requires EU members to ensure that obligations are imposed on a wide range of professionals, including auditors, attorneys, tax advisers, real estate agents and notaries.

Even if the United States does not adopt gatekeeper standards like those of the EU and the UK, the extraterritorial reach of several existing initiatives already subject lawyers who conduct international transactions to various requirements.

## INVESTMENT AND COMMODITY ADVISORS

Commodity futures and options accounts are vehicles that could be used to launder illicit funds. What are they?

- **Commodities:** Goods such as food, grains and metals that are usually traded in large amounts on a commodities exchange, usually through futures contracts.
- **Commodity pool:** Combines funds from various investors to trade in futures or options contracts.
- **Futures/futures contracts:** Contracts to buy or sell a set quantity of a commodity at a future date at a set price.
- **Options/options contracts:** Contracts that create the right, but not the obligation, to buy or sell a set amount of something, such as a share or commodity, at a set price after a set expiration date.
- **Omnibus accounts:** Accounts held by one futures commission merchant (FCM) for another.

Transactions of multiple account holders are combined and their identities are unknown to the holding FCM.

Commodity trading advisors (CTA) engage in the business of advising others, either directly or indirectly, as to the value or advisability of trading futures contracts, commodity options and/or swaps and issue analyses or reports concerning trading futures or commodity options. CTAs are also responsible for trading of managed futures accounts. By directing such accounts, CTAs are in a unique position to observe activity that may suggest money laundering. As such, they need to be aware of what types of activity may indicate potential laundering or terrorist financing and should implement compliance programs to detect and deter such activity.

Other positions with similar responsibilities are as follows.

- **Commodity pool operator:** Operator or solicitor of funds for a commodity pool, which combines funds from members and trades futures or options contracts.
- **Futures commission merchant (FCM):** A firm or person that solicits or accepts orders on futures contracts or commodity options and accepts funds for their execution.
- **Introducing broker-dealers in commodities (IB-Cs):** A firm or person that solicits and accepts commodity futures orders from customers but does not accept funds. There are two types of IB-Cs: guaranteed and independent.

- Guaranteed introducing broker: An introducing broker-dealer with an exclusive written agreement with a futures commission merchant that obligates the FCM to assume responsibility for the introducing broker's performance.
- Independent introducing broker: A broker that is subject to minimum capital and financial reporting requirements. This type of broker may introduce accounts to any FCM.
- Investment adviser: Provides advice on securities and investments and manages client assets.

Here are several ways this industry is susceptible to money laundering.

- Withdrawal of assets through transfers to unrelated accounts or to high-risk countries
- Frequent additions to or withdrawals from accounts
- Checks drawn on, or wire transfers from, accounts of third parties with no relation to the client
- Clients who request custodial arrangements that allow them to remain anonymous
- Transfers of funds to the adviser for management followed by transfers to accounts at other institutions in a layering scheme
- Investing illegal proceeds for a client
- Movement of funds to disguise their origin

## TRUST AND COMPANY SERVICE PROVIDERS

Trust and company service providers (TCSPs) participate in the creation, administration or management of corporate vehicles. They refer to any person or business that provides any of the following services to third parties.

- Acting as a formation agent of legal persons
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons
- Providing a registered office, business address or correspondence for a company, a partnership or any other legal person or arrangement
- Acting as (or arranging for another person to act as) a trustee of an express trust
- Acting as (or arranging for another person to act as) a nominee shareholder for another person

In a 2010 report called *Money Laundering Using Trust and Company Service Providers*, FATF found that in many jurisdictions the existence of TCSPs is not recognized. However, in these jurisdictions, trust and company services may well be provided by lawyers and other professionals who are already regulated. For example, in many jurisdictions, lawyers will be engaged in the formation of companies for clients to hold assets (e.g., a yacht, a residential or commercial property) outside of that client's jurisdiction. FATF noted that some TCSPs are required to afford confidentiality privileges to a client, which can conflict with AML reporting requirements.

Although the vast majority of companies and trusts are used for legitimate purposes, legal entities or other types of legal relationships formed by these professionals remain common to money laundering schemes.

The 2010 FATF report *Money Laundering Using Trust and Company Service Providers* provides the following vulnerabilities and red flags for this industry.

- Unknown or inconsistent application of regulatory guidelines regarding identification and reporting requirements
- Limited market restriction on practitioners to ensure adequate skills, competence and integrity
- Inconsistent record keeping across the industry
- Potential for TCSPs to operate in an unlicensed environment
- Potential for a TCSP's CDD to be performed by other financial institutions, depending on the jurisdictional requirements

Some potential indicators of money laundering for this industry include the following.

- Transactions that require the use of complex and opaque legal entities and arrangements
- The payment of consultancy fees to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies
- The use of TCSPs in jurisdictions that do not require TCSPs to capture, retain or submit to competent authorities information on the beneficial ownership of corporate structures formed by them
- The use of legal persons and legal arrangements established in jurisdictions with weak or absent AML/CFT laws and/or poor record of supervision and monitoring of TCSPs
- The use of legal persons or legal arrangements that operate in jurisdictions with secrecy laws
- Multiple intercompany loan transactions or multijurisdictional wire transfers that have no apparent or legal purpose

According to Transparency International, the reason to focus on service providers, rather than the company or trust, is that the latter are merely the tools through which the launderers operate. A company owned by criminals cannot protect itself, but service providers can, through diligence, reduce the risk of abusing the vehicles with which they have a relationship. That is why it is important that countries regulate service providers.

Regulations should stipulate how the service provider conducts its business, including how directors selected by the provider meet their obligations as trustees or trusteeships. In its 2004 report, Transparency International stated that the first jurisdiction to bring these activities under regulatory control was Gibraltar, which enacted legislation in 1989. Some other offshore jurisdictions either have introduced some form of regulatory control or will in the future.

Regulations are not uniform; they range from a simple minimum capitalization requirement to full regulatory oversight. Often, the scope of the legislation is limited, excluding certain types of activities. Sometimes, the legislation bars regulators from gaining access to client files without client permission (or a court order), thereby making checks on the adequacy of the license-holder's CDD provisions virtually impossible. Furthermore, although some jurisdictions include service providers within their AML regulations—for example, by making compliance with the regulations a condition of licensing—many do not, leaving service providers free of any AML duties beyond those imposed

upon the general public. As a result of these differing standards, it is easy for a person seeking to use a company or trust for criminal purposes to select a jurisdiction that either lacks requirements or has only inadequate ones, said Transparency International.

## REAL ESTATE

The real estate sector is frequently used in money laundering activities. Investing illicit capital in real estate is a classic method of laundering dirty money, particularly in countries with political, economic and monetary stability.

Escrow accounts, generally maintained by real estate agents and brokers and other fiduciaries, are designed to hold funds entrusted to someone for protection and proper disbursement. Countless real estate and business deals are closed every day using escrow funds. They are attractive to money launderers because of the large number of diverse transactions that can pass through them in any deal; escrow accounts can facilitate the movement of funds by cashier's checks, wire transfers or company checks to seemingly legitimate individuals or companies. Given the large amounts of activity that might be expected in an escrow account, a money launderer could easily disguise illegal activity in the account while appearing to operate the account in a manner consistent with what would be expected.

Many real estate transactions involve the deposit of a large check from the mortgagee, as well as checks and cash required from the buyer at closing (however, as discussed later in this section, cash purchases of real estate are becoming more prevalent). A money laundering title insurance agent can make multiple deposits of cash on a given day at several banks in amounts under the currency reporting threshold, credited to different, nonexistent closings. The deposits appear to be normal business activities, but they could very well represent the steady accumulation of funds for the purchase of real property by a person wishing to hide the origin of his funds. Ultimately, monies may be paid outright by the escrow agent as cashier's checks obtained by him, as wire transfers, or as corporate or escrow checks to straw men or shell corporations. Each closing also entails numerous routine disbursements for the payment of the proceeds to the seller, payoff of the mortgage, real estate commissions, taxes, satisfaction of liens and other payments. To a bank and other observers, the disbursement of funds at a closing may appear to be one legitimate set of transactions. Money laundering can be easily hidden because the size and volume of routine escrow account activity smooths out the spikes (i.e., the ups and downs in an account) or multiple deposits associated with money laundering.

In this industry we also see the reverse flip. A money launderer might find a cooperative property seller who agrees to a reported purchase price well below the actual value of the property and then accepts the difference under the table. This way, the launderer can purchase a \$2 million property for \$1 million, secretly passing the balance to the cooperative seller. After holding the property for a time, the launderer sells it for its true value of \$2 million.

In the loan back money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a loan or mortgage back to the trafficker for the same amount with all the necessary loan and/or mortgage documentation. This creates an illusion that the trafficker's funds are legitimate. The scheme is reinforced through legitimately scheduled payments made on the loan by the traffickers.

In April 2008, FinCEN published *Suspected Money Laundering in the Real Estate Industry*, an assessment based on suspicious activity report (SAR) filing analysis. The report makes a distinction between fraudsters and money launderers. Lenders are likely to file a SAR when they are the target of failed or successful mortgage fraud schemes that threaten the institution's revenues but may have significant difficulty detecting mortgage loan fraud perpetrated by money launderers. This is because money launderers strive to project the image of normalcy by integrating illicit funds through regular and timely payments. For example, only about 20 percent of SAR filings associated with the residential real estate industry reportedly described suspected structuring and/or money laundering.

In a 2015 brief, the Australian Transaction Reports and Analysis Centre (AUSTRAC) identified real estate to be a significant money laundering channel in Australia. The brief cites confiscations involving money laundering totaling over AUD\$23 million between 2012 and 2013. According to the brief, real estate is an attractive channel for laundering illicit funds because

- it can be purchased with cash;
- the ultimate beneficial ownership can be disguised;
- it is a relatively stable and reliable investment; and
- value may be increased through renovations and improvements.

Money laundering through real estate can be relatively uncomplicated compared to other methods and requires little planning or expertise. Large sums of criminal proceeds may be integrated into the legitimate economy through real estate investments (placement and layering phases). Properties may also be sold for a profit or retained for residential, investment or vacation purposes (integration phase).

In Australia, common money laundering methods involving real estate are as follows.

- Use of third party straw buyers described as cleanskins
- Use of loans and mortgages as a cover for laundering, which may involve lump sum cash repayments to integrate illicit funds into the economy
- Manipulation of property values to disguise undisclosed cash payments through over- or undervaluing or flipping through successive sales to increase value
- Structuring cash deposits used for the purchase
- Generation of rental income to legitimize illicit funds
- Conducting criminal activity, such as the production of cannabis or synthetic drugs, at the purchased property
- Use of illicit cash to make property improvements to increase the value and profits at sale
- Use of front companies, shell companies, trusts and other company structures to hide beneficial ownership and obvious links to criminals
- Use of gatekeepers, such as real estate agents, conveyancers or solicitors, to conceal criminal involvement, complicate the money laundering process and provide a veneer of legitimacy to the transaction

- Investment by overseas-based criminals to conceal assets and avoid confiscation from authorities in their home jurisdiction.

The report cites methods for detecting money laundering through real estate where transactions intersect with the regulated AML/CFT sector, such as when real estate transactions involve financial institutions in the form of loans, deposits or withdrawals. It also outlines red flags that should prompt further monitoring and examination, particularly when multiple indicators are present. These red flags include

- various uses of cash to aggregate funds for property purchase or down payment or to repay loans;
- multiple purchases and sales in a short period of time, sometimes involving property over- or under-valuation or straw buyers;
- use of offshore lenders;
- unknown sources of funds for purchase, such as incoming foreign wires where the originator and beneficiary customer are the same; and
- ownership is the customer's only link to the country in which the real estate is being purchased.

In its five-part Towers of Secrecy series published in 2015, *The New York Times* pierced the secrecy of more than 200 shell companies that have owned condominiums at the Time Warner Center, a high-end property located in the heart of Manhattan. In the investigative series, the newspaper found that nearly half of the most expensive residential properties are now purchased through shell companies throughout the United States. At the Time Warner Center, 37 percent of the condos are owned by foreigners, at least 16 of which have been the subject of governmental inquiries, including housing and environmental fraud. The foreign owners have included government officials and close associates of officials from Russia, Colombia, Malaysia, China, Kazakhstan and Mexico and they mainly used limited liability companies for the purchases. Oftentimes, signatures on the property documents were illegible, blank or signed by a lawyer with the lawyer's contact information registered.

The paper points out that there are no legal requirements for the real estate industry in the United States to identify beneficial owners or examine their backgrounds. In 2016 (subsequent to *The New York Times's* series), FinCEN began issuing a series of geographic targeting orders (GTOs) to help law enforcement identify individuals acquiring luxury residential properties through limited liability companies or other opaque structures without the use of bank financing. During the 180 days of each outstanding GTO, U.S. title insurance companies are required to identify the natural people behind shell companies used to pay all cash for high-end residential real estate in specified U.S. metropolitan areas that exceed specified dollar amounts prescribed for each area. It is important to note that in this context "all cash" refers to transactions that do not involve traditional financing and does not necessarily reference the use of physical cash.

## International Trade Activity

---

International trade activity is critical to an integrated economy and involves numerous components that can be manipulated for the benefit of money launderers and terrorist financiers, such as banks, currency exchange, free trade zones, cross-border payments, ports, invoices, goods, shipments, shell companies and credit instruments that oftentimes are inherently complex transactions. Trade-based money laundering and the black market peso exchange are two significant money laundering techniques that have proven successful in illicit finance. Typically, free trade zones are manipulated in both techniques.

### FREE TRADE ZONES

With more than 3,000 free trade zones (FTZs) in over 135 countries, FTZs play an integral role in international trade. FTZs are designated geographic areas with special regulatory and tax treatments for certain trade-related goods and services. FTZs are often located in developing countries near ports of entry but are separate from traditional ports of entry and typically operate under different rules. Most major FTZs are also located in regional financial centers that link international trade hubs with access to global financial markets. Examples of FTZs are the Colon Free Trade Zone in Panama and the Shanghai Free Trade Zone (officially the China Pilot Free Trade Zone) in China.

According to FATF's March 2010 *Report on the Money Laundering Vulnerabilities in Free Trade Zones*, systemic weaknesses for FTZs include

1. inadequate AML/CFT safeguards;
2. minimal oversight by local authorities;
3. weak procedures to inspect goods and legal entities, including appropriate record-keeping and information technology systems; and
4. lack of cooperation between FTZs and local customs authorities.

The relaxed oversight in FTZs makes it more challenging to detect illicit activity and provides an opportune setting for trade-based money laundering schemes. Moreover, FATF noted that some FTZs are as large as cities, which makes it difficult to effectively monitor incoming and outgoing cargo as well as repackaging and relabeling. Some FTZs export billions of dollars annually but have few competent authorities available to monitor and examine cargo and trade transactions.

### TRADE-BASED MONEY LAUNDERING TECHNIQUES

When men's briefs and women's underwear enter a country at prices of \$739 per dozen, missile and rocket launchers export for only \$52 each and full toilets ship out for less than \$2 each, one should notice the red flags. These manipulated trade prices represent money laundering, tax evasion and/or terrorist financing.

In a June 2006 report, called *Trade-Based Money Laundering*, FATF defined trade-based money laundering (TBML) as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can

be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

Money launderers can move money out of one country by simply using their illicit funds to purchase high-value products and then exporting them at very low prices to a colluding foreign partner, who then sells them in the open market at their true value. To give the transactions an air of legitimacy, the partners may use a financial institution for trade financing, which often entails letters of credit and other documentation.

The 2006 FATF study concluded that TBML represents an important channel of criminal activity and, given the growth of world trade, an increasingly important money laundering and terrorist financing vulnerability. Moreover, as the standards applied to other money laundering techniques become increasingly effective, the use of trade-based money laundering can be expected to become increasingly attractive.

According to the *Guidance Paper on Combating Trade-based Money Laundering*, February 1, 2016, developed by the Hong Kong Association of Banks with input from the Hong Kong Monetary Authority, understanding the commercial purpose of any trade transaction is a key requirement in determining its money laundering risk. The Guidance refers to six ways to execute trade-based money laundering:

1. **Overinvoicing or underinvoicing:**

- **Overinvoicing:** By invoicing the goods or service at a price above the fair market price, the seller is able to receive value from the buyer (i.e., the payment for the goods or service will be higher than the value that the buyer receives when it is sold on the open market).
- **Underinvoicing:** By invoicing the goods or service at a price below the fair market price, the seller is able to transfer value to the buyer (i.e., the payment for the goods or service is lower than the value that the buyer will receive when it is sold on the open market).

2. **Overshipping or short-shipping:** The difference in the invoiced quantity of goods and the quantity of goods that are shipped whereby the buyer or seller gains excess value based on the payment made

3. **Ghost-shipping:** Fictitious trades where a buyer and seller collude to prepare all the documentation indicating goods were sold, shipped and payments were made, but no goods were actually shipped

4. **Shell companies:** Used to reduce the transparency of ownership in the transaction

5. **Multiple invoicing:** Numerous invoices issued for the same shipment of goods, thus allowing the money launderer the opportunity to make numerous payments and justify them with the invoices

6. **Black market trades:** Commonly referred to as the Black Market Peso Exchange, whereby a domestic transfer of funds is used to pay for goods by a foreign importer

Letters of credit are another vehicle for money laundering. Letters of credit are a credit instrument issued by a bank that guarantees payments on behalf of its customer to a third party when certain conditions are met. Letters of credit are commonly used to finance export because exporters want assurance that the ultimate buyer of its goods will make payment, and this is given by the buyer's purchase of a bank letter of credit. The letter of credit is then forwarded to a correspondent bank in the jurisdiction in which the payment is to be made. The letter of credit is drawn on when the goods are loaded for shipping, received at the importation point, clear customs and are delivered. Letters of credit can be used to facilitate money laundering by transferring money from a country with lax exchange controls, thus assisting in creating the illusion that an import transaction is involved. Moreover, letters of credit can also serve as a façade when laundering money through the manipulation of import and export prices. Another method of using letters of credit illicitly is in conjunction with wire transfers to bolster the legitimate appearance of nonexistent trade transactions.

In July 2012, the Asia/Pacific Group on Money Laundering (APG) issued the *APG Typology Report on Trade Based Money Laundering*, which reaffirmed the conclusions of the 2006 FATF study. The APG study cited the lack of reliable statistics relating to TBML as a major obstacle in devising strategies to tackle it. To assist in recognizing the multiple forms of TBML, the paper enumerates specific characteristics and red flags associated with jurisdictions, goods, corporate structures and predicate offenses.

It concluded that any strategy to prevent and combat TBML needs to be based on dismantling TBML structures, while allowing genuine trade to occur unfettered. It calls for an integrated, holistic approach, with an emphasis on interagency coordination and international cooperation to standardize data and statistics, create domestic task forces, deliver TBML-focused training and conduct further research.

### Case Study

In February 2011, the U.S. Department of the Treasury designated the Lebanese Canadian Bank (LCB) as a financial institution of primary money laundering concern, asserting that Hezbollah derived financial support from drug and money laundering schemes, including TBML. The TBML component of the operations involved consumer goods worldwide, including used cars purchased in the United States and shipped to West Africa for resale, with a portion of the proceeds allegedly funneled to Hezbollah.

In May 2014, FinCEN issued an advisory on the use of funnel accounts and trade-based money laundering. The advisory was the result of the possible impact of the 2010 Mexican law that restricted cash deposits of U.S. dollars in Mexican banks. Subsequently, the restrictions were expanded to include similar deposits made at exchange houses (*casas de cambio*) and brokerages (*casas de bolsa*) in Mexico. Furthermore, additional guidance was issued by FinCEN based on bulk cash smuggling trends based on the restrictions that indicated an increase in the use of funnel accounts to move illicit proceeds of Mexico-related criminal organizations.

FinCEN defines a funnel account as “an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.” Ways to identify possible funnel account activity include the following.

- An account opened in one U.S. state receives numerous cash deposits of less than \$10,000 (the currency reporting requirement) by unidentified persons at branches outside of the geographic region where the account is domiciled.
- Business account deposits take place in a different geographic region from where the business operates.
- Individuals opening or making deposits to funnel accounts lack information about the stated activity of the account, the account owner or the source of the cash.
- A business account receives out-of-state deposits with debits that do not appear to be related to its business purpose.
- There are notable differences between the handwriting on the payee and amount lines and the signature line on checks issued from an account that receives out-of-state cash deposits.
- Wire transfers or checks issued from a funnel account are deposited into, or cleared through, the U.S. correspondent account of a Mexican bank.

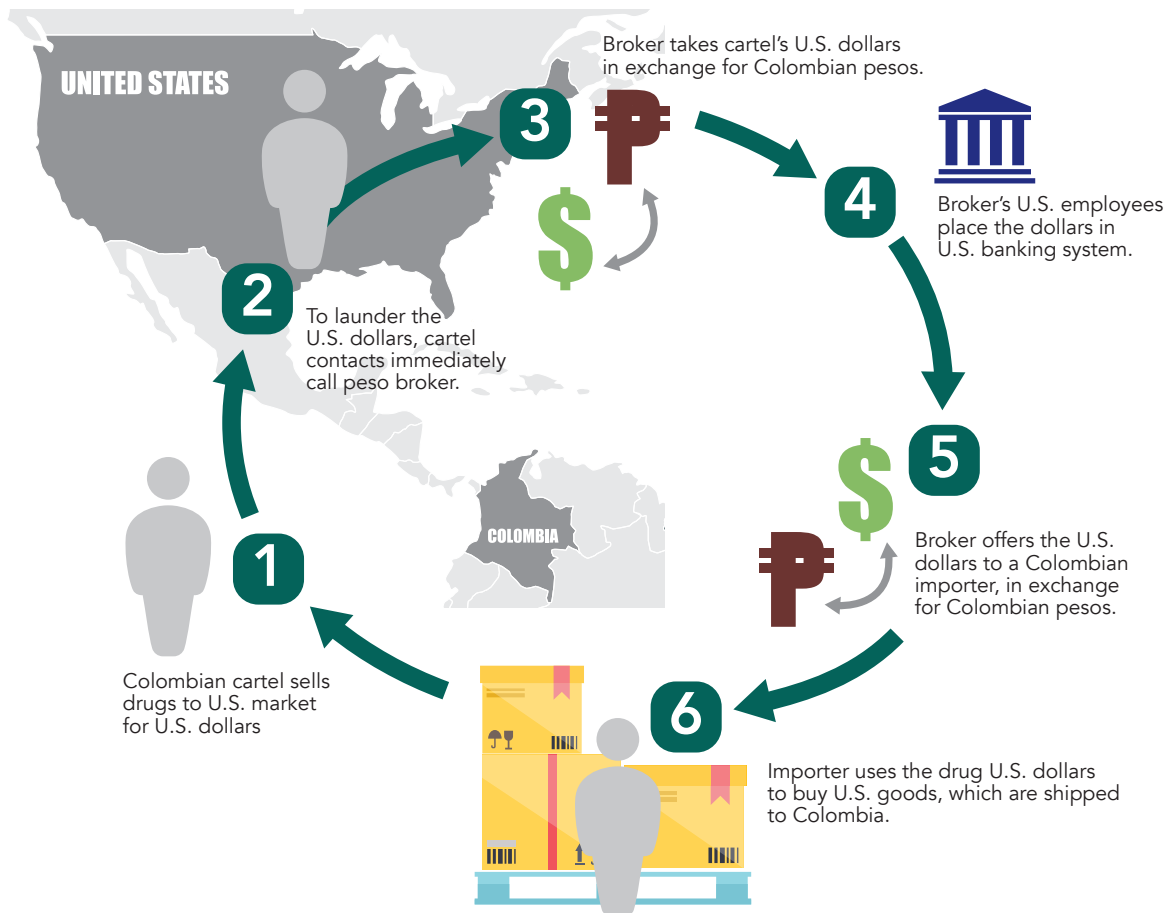
## BLACK MARKET PESO EXCHANGE

A form of trade-based money laundering, the Black Market Peso Exchange (BMPE) is a process by which money in the United States derived from illegal activity is purchased by Colombian peso brokers and deposited in U.S. bank accounts that the brokers have established. The brokers sell checks and wire transfers drawn on those accounts to legitimate businesses, which use them to purchase goods and services in the United States. Although the United States is prominently figured in BMPE, the process is not limited exclusively to it.

Colombian importers created the BMPE in the 1950s as a mechanism for buying U.S. dollars on the black market to avoid domestic taxes and duties on the official purchase of U.S. dollars and on imported goods purchased with dollars. In the 1970s, Colombian drug cartels began using the BMPE to convert drug dollars earned in the United States to pesos in Colombia. Why? It reduced their risk of losing their money through seizures and they got their money faster, even though they paid a premium to the peso broker.

In FinCEN's February 18, 2010 *Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering*, it indicated that black market currency exchange systems have evolved beyond the Colombian BMPE method, mainly because of increased diligence by U.S. banks. A common method used for initial placement of illicit funds into the financial system was structured deposits in the form of cash, money orders or other financial instruments. However, money launderers are currently utilizing individuals or businesses that have control over numerous bank accounts at numerous banks to smuggle cash in bulk from the United States. The smuggled U.S. dollars are deposited into foreign institutions—often in Mexico, but also in Central and South American countries—and wired back to the United States and other prominent trade countries as payments for international trade goods and services.

## Black Market Peso Exchange Example



According to the U.S. Department of Justice in its April 24, 2014 press release on the prison terms for the owners of an import-export company that was used to move millions of dollars linked to illegal activity from the United States to Mexico, the following is a typical BMPE scenario involving the United States and Mexico:

A peso broker works with an individual engaged in illegal activity, such as a drug trafficker, who has U.S. currency in the United States that he needs to bring to Mexico and convert to pesos. The peso broker finds business owners in Mexico who buy goods from vendors in the United States, such as XYZ Inc., and need dollars to pay for those goods. The peso broker arranges for the illegally obtained dollars in the United States to be delivered to the U.S.-based vendors, such as XYZ Inc., where they are used to pay for the goods purchased by the Mexico based customers. Once the goods are shipped to Mexico and sold by the Mexico-based business owner for pesos, the pesos are turned over to the peso broker, who then pays the drug trafficker in Mexico.

### Case Study

In September 2014, extensive law enforcement operations revealed evidence of pervasive money laundering activities involving BMPE schemes throughout the Los Angeles, California Fashion District. The area includes over 2,000 businesses covering about 100 city blocks in downtown Los Angeles. Garment industry businesses in the fashion district were used to launder money for drug trafficking organizations (DTOs). Bulk cash proceeds from drug sales were used to purchase textile-related goods, which were shipped to Mexico and other countries. The proceeds from the sales of the exported goods were forwarded to the DTOs in the form of local currency. During the September 10, 2014, enforcement action, U.S. Homeland Security Investigation special agents seized over \$90 million in currency, the largest single-day bulk cash seizure in U.S. history. The seized cash was found at various residences and businesses stored in various places, such as file boxes, duffel bags, backpacks and even in the trunk of a Bentley. FinCEN issued a geographic targeting order (GTO) on September 26, 2014, that lowered cash thresholds and triggered additional record-keeping requirements on specified textile-related businesses in the LA Fashion District in an effort to disrupt the activities of DTOs.

### Case Study

In April 2015, FinCEN issued a GTO that similarly lowered cash reporting thresholds and implemented additional record-keeping requirements for certain financial transactions for about 700 Miami-based electronics exporters. According to FinCEN, the GTO was designed to disrupt complex BMPE-related schemes employed by DTOs, including the Sinaloa and Los Zetas DTOs based in Mexico. Law enforcement investigations revealed that many of these businesses are exploited by sophisticated TBML/BMPE schemes in which drug proceeds in the United States are converted into goods that are shipped to South America and sold for local currency and ultimately transferred to drug cartels. The GTO was designed to enhance the transparency of the covered businesses' transactions.

## **Risk Associated With New Payment Products and Services**

---

The Internet, new payment platforms and electronic money have changed the way people conduct business and transact with each other, as well as how consumers buy products and services. Whereas a small corner shop was limited to servicing local consumers, it can now have a broader, global reach with an online business as well. Digital payment platforms have altered how a consumer and the regulatory environment view a merchant or funds transmission. The cheaper cost of technology and our globally interdependent society, increasingly highly skilled engineering-based workforce and entrepreneurial drive have all contributed to the evolution of new payment products and services pushing the boundaries of how and where money is used. Generally, the risk posed by these new payment systems is relative to the functionality of the service and their funding mechanisms.

## Prepaid Cards, Mobile Payments and Internet-Based Payment Services

---

In October 2006, FATF published a report that examined the ways in which money can be laundered through the exploitation of new payment methods, such as prepaid cards, Internet payment systems, mobile payments and digital precious metals. The report found that, although there is a legitimate market demand for these payment methods, money laundering and terrorist financing vulnerabilities exist. In addition, cross-border providers of new payment methods may pose more risk than providers operating just within a particular country. The report recommended continued vigilance to further assess the impact of evolving technologies on cross-border and domestic regulatory frameworks.

Prepaid cards have the same characteristics that make cash attractive to criminals: they are portable, valuable, exchangeable and anonymous. Typically, prepaid products require the consumer to pay in advance for future purchases of goods and services. Each payment is subtracted from the balance of the card or product until the total amount is spent. Prepaid cards can be categorized as either open loop or closed loop. Open-loop prepaid cards, many of which are network branded by American Express, Visa or MasterCard, can be purchased and loaded with money by one person and used like regular debit cards by the same person or another person to make purchases or ATM withdrawals anywhere in the world. Closed-loop prepaid products are of limited use for a specific purpose or service, such as with a certain merchant or retailer, whether online or at a physical location. A prepaid card may be either nonreloadable, which means it is purchased for a fixed amount that cannot be reloaded as the funds are depleted, or reloadable, which permits adding funds on the card to replace what was previously spent.

Although there are many different types of prepaid cards that are used in a variety of ways, the cards typically operate in the same way as a debit card and ultimately rely on access to an account. There may be an account for each card that is issued or, alternatively, there may be a pooled account that holds the prepaid funds for all cards issued. The cards may be issued by, and accounts may be held at, a depository institution or a nonbank organization; pooled accounts would be normally held by the issuer at a bank.

The report identified these potential risk factors with prepaid cards.

- Anonymous cardholders
- Anonymous funding
- Anonymous access to funds
- High value limits and no limits on the number of cards individuals can acquire
- Global access to cash through ATMs
- Offshore card issuers that may not observe laws in all jurisdictions
- Substitute for bulk-cash smuggling

Electronic purses (also called e-purses or stored-value or smart cards) are cards that electronically store value on integrated circuit chips. Unlike prepaid credit cards with magnetic stripes that store account information, e-purses actually store funds on memory chips.

Measures associated with these payment methods that might limit the vulnerability to money laundering are as follows.

- Limiting the functions and capacity of the cards (including the maximum value and turnover limits, as well as the number allowed per customer)
- Linking new payment technology to financial institutions and bank accounts
- Requiring standard documentation and record-keeping procedures for these systems to facilitate their examination
- Allowing for the examination and seizure of relevant records by investigating authorities
- Establishing international standards for these measures

According to the Joint Money Laundering Steering Group's guidance on electronic money (2012), electronic money is "a prepaid means of payment that can be used to make payments to multiple persons, where the persons are distinct legal or natural entities." Electronic money products can be card-based or online account-based. They can be issued by banks, building societies and specialist electronic money institutions. Examples of e-money include prepaid cards that can be used to pay for goods at a range of retailers or virtual purses that can be used to pay for goods or services online. All UK e-money institutions are regulated by the UK Financial Conduct Authority (FCA) and are governed under the Electronic Money Regulations (2011), which require compliance with all AML/CFT and sanctions requirements.

The guidance identifies several risk factors inherent in e-money for money laundering and terrorist financing, including

- high, or no, transaction limits;
- frequent cross-border transactions;
- certain merchant activity with higher risk businesses, such as gambling;
- funding with unverified persons;
- funding with cash that leaves no electronic trail to the source of funds;
- funding with other electronic money that lacks verified persons and/or source of funds;
- non-face to face transactional activity;
- features that increase the functionality of the card in terms of how to execute transactions, such as person to person, business to person, business to business, person to business;
- ability of customer to hold numerous purses; and
- segmentation of the business value chain.

After the 2006 typology report, FATF issued a similar report in 2010. And as the market continued to evolve, FATF issued *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, in 2013. In the guidance, FATF identified numerous inherent risks with what it called new payment methods (NPMs). They are as follows.

- **Non-face-to-face relationships and anonymity**
  - NPMs can be used to quickly move funds around the world, to make purchases and to give access to cash through the ATM network.
  - For prepaid cards, anonymity can occur when the card is purchased, registered, loaded, reloaded or used.
  - Prepaid cards can easily be passed on to third parties that are unknown to the issuer.
  - Customers may be established through agents, online or through a mobile payment system.
  - There is an increase in the risk of identity fraud or customers providing inaccurate information potentially to disguise illegal activity in non-face-to-face verification.
- **Geographical reach**
  - Open-loop prepaid cards usually permit payments at domestic and foreign points of sales through global payment networks.
  - Prepaid card providers may be based in one country and sell their product internationally through agents or online.
  - The compact size of prepaid cards makes them more vulnerable to misuse than cash in cross-border transportations.
  - Mobile and online payment services can transfer funds globally.
  - Different regulatory AML/CFT regimes may exist where payments originate versus where they are ultimately received.
- **Methods of funding**
  - Prepaid card risk is increased by allowing cash funding and the possibility of reloading without any limit on the value placed on the card.
  - Use of prepaid cards is an alternative to the physical cross-border transportation of cash.
  - Mobile and online payment services can be funded using numerous methods, such as banks account, or nonbank methods, including money transmitters, electronic monies and virtual currencies.
- **Access to cash**
  - ATM networks may be used for prepaid cards that allow funding in one country and cash withdrawals in another.
  - There is increasing connectivity between mobile and online payment methods with prepaid cards to fund or withdraw in cash.
- **Segmentation of services**
  - Prepaid cards usually require several parties to execute transactions, including the program manager, issuer, acquirer, payment network, distributor and agents.

- Mobile and online services require coordination with numerous interrelated service providers who must partner with international counterparts to provide cross-border transactions.
- Customer acquisition may rely on unaffiliated third parties or the use of agents.
- NPM providers maintain bank accounts and use the banking system for periodic transactions to settle accounts with agents or partners, and the banks may not have visibility into the ultimate customer for the transaction.

The guidance also stated that the risk of money laundering and terrorist financing in NPMs may be mitigated when the following are considered.

- **Customer due diligence (CDD)**

- The need for CDD and the extent to which it should be performed varies depending on the level of risk posed by the product.
- The greater the functionality of the NPM, the greater the need may be for more enhanced CDD.
- Customer information in non-face-to-face verification may be corroborated using third party databases but also using open-source information readily available on the Internet or social media.

- **Loading, value and geographical limits**

- Set initial load limits.
- Set geographical or reloading limitations.
- Limit the functionality of a product to certain geographical areas.
- Limit the functionality of a product to the purchase of certain goods and services.
- Consider establishing individual tiers of service provided to customers.
- For prepaid cards
  - > Put limits on loading, duration and ability to make cash withdrawals.
  - > Limit the amount that is prepaid and accessible.
- For mobile
  - > Set a maximum amount allowed per single transaction.
  - > Set a maximum for cash withdrawals.
  - > Limit the frequency or cumulative value of transactions.
  - > Set limits based on the day, week, month, year or a combination thereof.

- **Source of funding:**

- Consider limited allowable sources of funding for a specific product.
- Consider identification for cash-based funding depending on load or account limits.

- **Record keeping, transaction monitoring and reporting**
  - Retain transaction records of payments and funds transfers.
  - Retain identifying information on the parties to the transaction.
  - Retain and identify any account(s) involved.
  - Retain the date of the transaction and the amount involved.
  - For mobile, obtain the phone number of the sender and receiver.
  - Implement and utilize transaction monitoring-relevant typologies.

## Virtual Currency

---

A virtual or digital currency (VC) is a medium of exchange that operates in the digital space. It can either be converted into a fiat (e.g., a government-issued currency) or it can be a substitute for real currency. There are two types of virtual currencies: centralized and decentralized. Centralized virtual currencies (e.g., formerly the Liberty Reserve) have a centralized repository and a single administrator. Decentralized (e.g., Bitcoin) VCs have no repositories or administrators but work as peer-to-peer media of exchange without any need for an intermediary. According to FATF's 2014 report *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, VCs can also be distinguished between convertible VCs (i.e., Bitcoin and WebMoney) that have an equivalent value and can be exchanged in real currency and non-convertible VCs (i.e., Q Coins and World of Warcraft Gold) that are intended to be specific to a particular domain.

Virtual currencies allow value to be able to be transmitted anywhere in the world without the requirement of a centralized bank or institutional authority. In 2009, the Bitcoin ecosystem was developed as a cryptographic protocol to transfer value through the peer-to-peer network without reliance on a centralized banking structure. Bitcoins are units of value transfer that are established as a virtual currency. Much like any financial instrument, a Bitcoin derives its value from what another party is willing to trade for that item. In the case of Bitcoins, there is a value that is expressed in fiat currency that is based upon economic and market forces. A Bitcoin can be expressed as an equivalent value in each locale's specific currency.

With the VC market gaining traction and an increase in individuals and businesses operating in the ecosystem, on March 18, 2013, FinCEN issued interpretative guidance on VCs that categorized the participants within the ecosystem into three segments.

- A User is a person who obtains virtual currency to purchase goods or services.
- An Exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency.
- An Administrator is a person engaged as a business in issuing a virtual currency and who has the authority to redeem such virtual currency.

The guidance states that Administrators or Exchangers of virtual currency are MSBs engaging in money transmission and must comply with the registration, reporting, record-keeping and other regulations applicable to money transmitters, such as maintaining a compliant AML program.

In a typical transaction scenario, a User has an established virtual wallet or an account with an Exchanger to conduct a transaction. The User acquires virtual currency from the Exchanger, which allows the User to transfer funds in and out of that account. In relation to Bitcoin, in a transfer between two individuals, no personally identifiable information is disclosed to the two individuals or to any third-party intermediaries. Although each transaction is registered in the blockchain and the publicly available distributed ledger, which provides valuable information beyond a traditional cash-to-cash exchange, it does not provide the actual identities behind the corresponding wallets. Thus, know your customer (KYC) is an important component of a legitimate exchanger's AML program.

For those tracking the movement of illicit funds, ownership information may be unavailable, with only the wallet address of the previous sender provided. However, the underlying technology and public recording of transactions allows for wallet address association that assists investigators in piecing together the ownership puzzle. VC businesses that facilitate the use, purchase and transfer of VCs are an important source for details related to wallet ownership and source of fund information.

The regulation of VC businesses varies globally, ranging from AML/CFT obligations for exchanges to the mere issuance of advisories to the financial sector on the risks posed by those businesses as customers. In some countries, the financial sector is prohibited from interacting with VC businesses entirely.

### Case Study

Liberty Reserve was a web site out of Costa Rica that used digital currency (its own called LR) for payment processing and money transmission. In May 2013, FinCEN issued a Notice of Finding under Section 311 of the USA PATRIOT Act that Liberty Reserve S.A. was a financial institution of primary money laundering concern. Later that month, the United States shut down the website. At the time, Liberty Reserve had more than 5.5 million user accounts worldwide and had processed more than 78 million financial transactions with a combined value of more than \$8 billion.

Liberty Reserve maintained more than 200,000 customers in the United States, yet never registered with FinCEN as an MSB. Liberty Reserve did not conduct verification of account registration for individuals using the system, asking only for a working email address, and allowed an individual to open an unlimited number of accounts. By paying an additional privacy fee, users could hide their internal unique account number when sending funds within the Liberty Reserve system. Once an account was established, Liberty Reserve virtual currency could be sent instantly and anonymously to any other account holder within the global system. Essentially, unverified account holders could use the site to transfer LR between other unverified accounts holders.

Accounts were funded using exchangers, third-party entities that maintained bulk quantities of LR that were purchased using traditional funding methods. The exchangers operated as unlicensed money transmitters. Technically, the design was to layer funds from the point of origin (traditional funding, such as cash or wire transfers) through the exchangers into a digital currency, and then the digital currency could be used to purchase illicit goods or withdrawn out of Liberty Reserve using a different exchanger. In May 2016, the founder, Arthur Budovsky, was sentenced to 20 years in prison for running the money laundering enterprise. Four codefendants pleaded guilty and two of the remaining conspirators remain at large.

### Case Study

In September 2013, the U.S. Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a dark market website created in 2011 to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking and money laundering conspiracies. Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers. In May 2015, Ross Ulbricht was sentenced in Manhattan federal court to life in prison in connection with his operation and ownership of the site. Bitcoin was the sole accepted currency on the Silk Road.

## **Corporate Vehicles Used to Facilitate Illicit Finance**

---

Various forms of corporate vehicles exist and are used to facilitate the movement of illicit finance. For example, corporate vehicles can be misused for money laundering, bribery and corruption activity, sheltering assets and tax evasion, among other uses. Vehicles such as corporations, partnerships and trusts are all excellent methods to maximize anonymity of ownership as well as its actual purpose.

## **Public Companies and Private Limited Companies**

---

In most jurisdictions, corporate structure is distinguished between public companies and private limited companies. For public companies, shares are freely available and traded publicly, there is usually no limit to the number of shareholders, information on ownership and its board of directors is publicly available and the companies are subject to significant regulation. On the other hand, private limited companies are not publicly traded, are restrictive in the number of shares, have ownership that can be by one or many and are subject to minimal regulatory oversight.

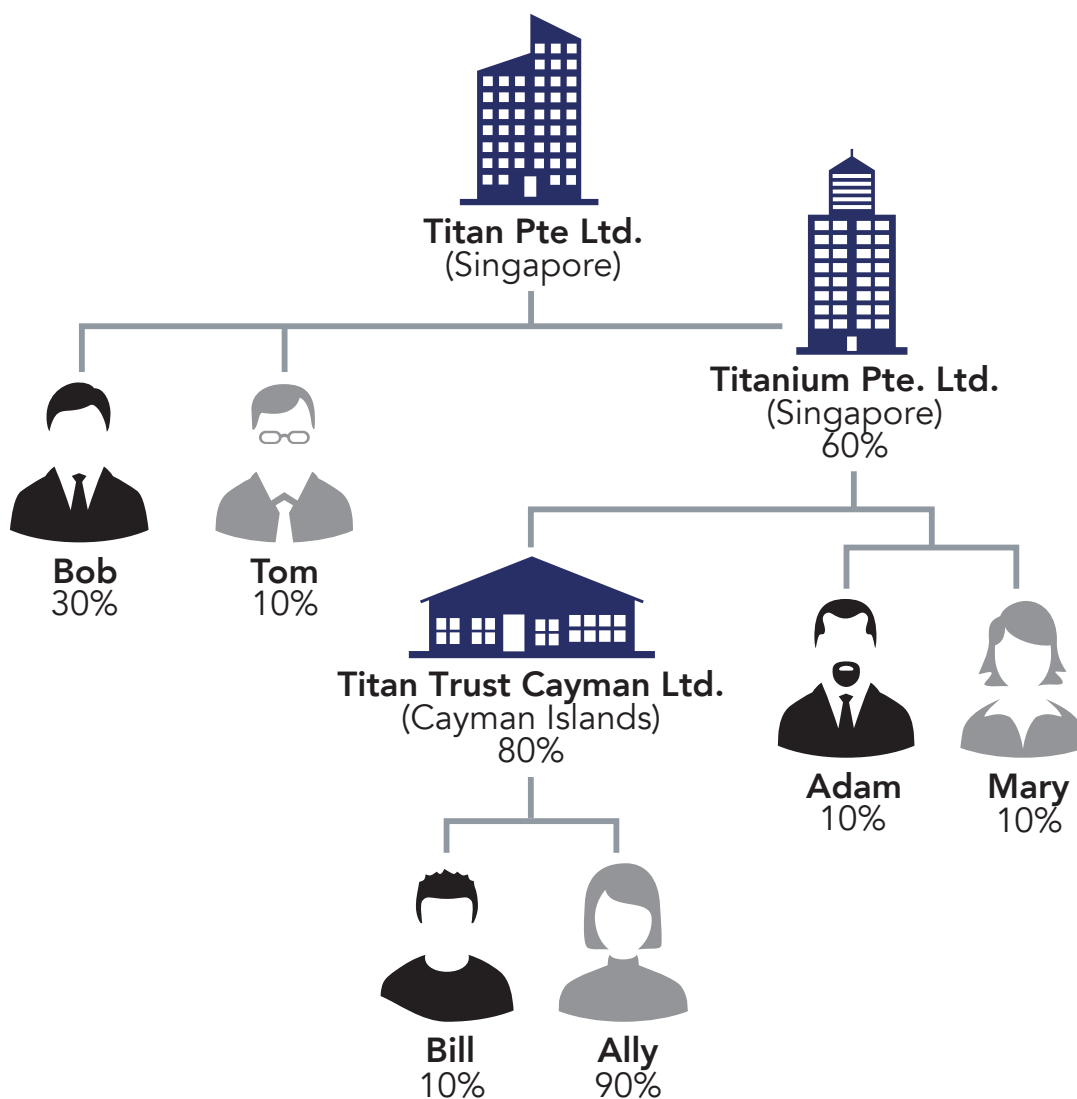
A very common corporate vehicle subject to misuse is the limited liability company (LLC). The LLC is an attractive vehicle because LLCs can be owned or managed anonymously; virtually anyone can own or manage an LLC, including foreign persons and other business entities.

A member of an LLC is equivalent to a shareholder in a corporation. A manager, on the other hand, is equivalent to an executive officer or a member of the board of directors. An LLC may lack managers, in which case the members manage the LLC. FinCEN has undertaken a number of activities to monitor LLCs better, because not every state (especially U.S. domestic LLCs) is undertaking the same measures and controls towards LLCs (especially in the monitoring, recording and reporting of managers, ultimate beneficiaries and nominees).

International business corporations (IBCs) are entities formed outside of a person's or business's country of residence, typically in offshore jurisdictions, for confidentiality or asset protection purposes. IBCs permit the person to reduce transparency between the owner in his or her home country and the offshore entity where the company is registered. As a result, some benefits include asset

protection, access to multiple investment markets, estate planning, legitimate tax benefits and serving as holding companies. The inherent risks with IBCs are that they are usually created in a tax haven and they usually require incorporation with a local agent, who may further reduce the transparency of the IBC (e.g., serving as a nominee owner or director) and facilitate opening accounts in the name of the IBC. Private investment companies (PICs) are established and used in a similar manner; however, they are typically limited to holding investment assets in tax-neutral offshore financial jurisdictions.

## Corporate Vehicles Example



## BEARER SHARES IN CORPORATE FORMATION

Bearer bonds and bearer stock certificates or bearer shares are prime money laundering vehicles because they belong on the surface to the bearer. When bearer securities are transferred, because there is no registry of owners, the transfer takes place by physically handing over the bonds or share certificates. Basically, the person who holds the bonds or shares gets to claim ownership.

Bearer shares offer lots of opportunities to disguise their legitimate ownership. To prevent this from happening, FATF in its 40 Recommendations suggested that employees of financial institutions ask questions about the identity of beneficial owners before issuing, accepting or creating bearer shares and trusts. Financial institutions should also keep registries of this information and share it appropriately with law enforcement agencies.

Several FATF members do allow the issuance of bearer shares and maintain that they have legitimate functions in facilitating the buying and selling of such securities through book entry transfers. They also can be used, according to some sources, for concealing ownership for tax optimization purposes.

Bearer checks are unconditional orders (negotiable instruments) that, when presented to a financial institution, must be paid out to the holder of the instrument rather than to a payee specified on the order itself. Bearer checks are used in a number of countries. The financial institution is usually not obligated to verify the identity of the presenter of a bearer check unless the transaction exceeds a particular threshold. A non-bearer check may become a bearer instrument, payable to the individual who presents it, when the original payee has endorsed it.

## Shell and Shelf Companies

---

Although shell companies may be created for legitimate purposes, they can also be established with the primary objective to claim the proceeds of crime as legitimate revenue and/or to commingle criminal proceeds with legitimate revenue. The use of shell and shelf companies to facilitate money laundering is a well-documented typology, according to FATF. FATF offers the following definitions.

- **Shelf company:** A corporation that has had no activity. It has been created and put on the shelf. This corporation is then later sold to someone who prefers a previously registered corporation over a new one.
- **Shell company or corporation:** A company that at the time of incorporation has no significant assets or operations.

In October 2006, FATF issued a report called *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers*. In this report, FATF said that of particular concern was the ease with which corporate vehicles can be created and dissolved in some jurisdictions. It allows these vehicles to be used not only for legitimate purposes (such as business finance, mergers and acquisitions or estate and tax planning) but also by those involved in financial crime to conceal the sources of funds while keeping their ownership concealed.

Shell companies can be set up in onshore as well as offshore locations and their ownership structures can take several forms. Shares can be issued to a natural or legal person or in registered or bearer form. Some companies can be created for a single purpose or to hold a single asset. Others can be established as multipurpose entities. Shell companies are often legally incorporated and registered by the criminal organization but have no legitimate business. Often purchased “off the shelf” from lawyers, accountants or secretarial companies, they are convenient vehicles to launder money. Sometimes, the stock of these shell corporations is issued in bearer shares, which means

that whoever carries them is the purported owner. Tax haven countries and their strict secrecy laws can further conceal the true ownership of shell corporations. In addition, the information may be held by professionals who claim secrecy.

When FATF reviewed the rules and practices that impair the effectiveness of money laundering prevention and detection systems, it found in particular that shell corporations and nominees are widely used mechanisms to launder the proceeds from crime. A 2001 report, *Money Laundering in Canada: An Analysis of RCMP Cases*, offered four related reasons to establish or control a shell company for money laundering purposes:

1. Shell companies accomplish the objective of converting the cash proceeds of crime into alternative assets.
2. Through the use of shell companies, the launderer can create the perception that illicit funds have been generated from a legitimate source. Once a shell company is established, commercial accounts can be created at banks or other financial institutions. Especially attractive to money launderers are businesses that customarily handle a high volume of cash transactions, such as retail stores, restaurants, bars, video arcades, gas stations or food markets. Illicit revenues can then be deposited into bank accounts as legitimate revenue, either alone or commingled with revenue legitimately produced from the business. Companies also offer criminals legitimate sources of employment in the community, which in turn helps cultivate an image of respectability.
3. Once a shell company is established, a wide range of legitimate and/or bogus business transactions can be used to further the laundering process. These include lending money between criminally controlled firms, paying out fictitious expenses or salaries, disguising the transfer of illicit funds under the guise of payment for goods or services or purchasing real estate with the proceeds of crime or disguising payments for real estate as mortgages issued by a shell company. As a medium between criminal organizations and other laundering vehicles, shell companies are flexible and can be tailored to a launderer's specific needs. For example, criminal organizations laundering money through real estate can incorporate real estate agencies, mortgage-brokerage firms and development or construction companies to facilitate access to real property.
4. Shell companies can also be effective in concealing criminal ownership. Nominees can be used as owners, directors, officers or shareholders. Companies in one country can also be incorporated as subsidiaries of corporations based in another country (especially a tax haven country with strict secrecy and disclosure laws), thereby greatly inhibiting investigations into their ownership. Shell companies can also be used to hide criminal ownership in assets, by registering these assets, such as real estate, in the name of a company.

Criminal enterprises also use real businesses to launder illicit money. These businesses differ from shell companies in that they operate legitimately, offering industrial, wholesale or retail goods or services. The Canadian report mentions the following money laundering techniques used in conjunction with criminally controlled companies.

- **Using nominees as owners or directors:** To distance a company from its criminal connections, nominees will be used as company owners, officers and directors. Nominees will often, but not necessarily, have no criminal record. Further, companies established by lawyers will often be registered in the lawyers' name.

- **Layering:** In some cases, a number of companies are established, many of them connected through a complex hierarchy of ownership. This helps to conceal criminal ownership and facilitates the transfer of illicit funds between companies, muddying any paper trail.
- **Loans:** Proceeds of crime can be laundered by lending money between criminally-controlled companies. In one case, a drug trafficker had \$500,000 in a bank account in the name of a shell company. These funds were lent to restaurants in which the drug trafficker had invested. This seemingly legitimate use of the funds assisted in making it appear that the funds were being properly integrated into the economy. The \$500,000 was repaid with interest to avoid suspicion.
- **Fictitious business expenses/false invoicing:** Once a criminal enterprise controls corporate entities in different jurisdictions, it can employ a laundering technique known as double invoicing. An offshore corporation orders goods from its subsidiary in another country, and the payment is sent in full to the bank account of the subsidiary. Both companies are owned by the criminal enterprise and the payment for goods is actually a repatriation of illicit money previously spirited out of the country. Moreover, if the subsidiary has charged a high price for the goods, the books of the parent company will show a low level of profit, which means that the parent company will pay less in taxes. It can also work the other way around. An offshore corporation buys goods from a parent company at price that is too high. The difference between the real price and the inflated price is then deposited in the subsidiary's account.
- **Sale of the business:** When the criminal sells the business, he has a legitimate source of capital. The added benefit of selling a business through which illicit money circulates is that it will ostensibly exhibit significant cash flow and, as such, will be an attractive investment and will realize a high selling price.
- **Buying a company already owned by the criminal enterprise:** An effective laundering technique is to purchase a company already owned by the criminal enterprise. This laundering method is most frequently used to repatriate illicit money that was previously secreted to foreign tax havens. Criminal proceeds from offshore are used to buy a company that is already owned by the criminal enterprise. In this way, the launderer successfully returns a large sum of money that had been secreted out of the country.
- **Paying out fictitious salaries:** In addition to claiming the proceeds of crime as legitimate business revenue, criminally-controlled companies also help make certain participants in a criminal conspiracy appear to be legitimate by providing them with salaries.

---

## Trusts

Trusts are private fiduciary arrangements that allow a grantor, or settlor, to place assets for future distribution to beneficiaries. The grantor/settlor will usually appoint a third party, a trustee, to administer the assets in accordance with the instructions provided in the trust document. Trusts are often seen as separate legal entities from the grantor; as such, they are often useful for estate planning and asset protection purposes. The instructions usually state how the grantor/settlor would like the funds to be distributed and are limited only to a legal purpose.

Trusts fall into one of two categories: revocable, in which case the grantor/settlor can terminate the trust, or irrevocable, in which case the grantor cannot terminate the trust once created. The flow of funds from the trust assets (the principal) to the beneficiaries can be in any of a number of ways, including providing them with the income generated by the principal, by providing fixed distributions of interest and/or principal or putting conditions on distributions (e.g., completing certain levels of schooling). Trusts will also name remaindermen who are designated to receive any residual assets after the conclusion of the trust's term (e.g., after the death of the grantor or the beneficiaries). Trusts allow a significant amount of flexibility and protection and have been used legitimately for centuries.

The significance of a trust account—whether onshore or offshore—in the context of money laundering cannot be understated. It can be used in the first stage of converting illicit cash into less suspicious assets; it can help disguise the criminal ownership of funds or other assets; and it is often an essential link between different money laundering vehicles and techniques, such as real estate, shell and active companies, nominees and the deposit and transfer of criminal proceeds.

In some jurisdictions, trusts may be formed to take advantage of strict secrecy rules in order to conceal the identity of the true owner or beneficiary of the trust property. They are also used to hide assets from legitimate creditors, to protect property from seizure under judicial action or to mask the various links in the money flows associated with money laundering or tax evasion schemes. For example, asset protection trusts (APTs) are a special form of irrevocable trust usually created (i.e., settled) offshore for the principal purposes of preserving and protecting part of one's wealth from creditors. Title to the asset is transferred to a person named the trustee. APTs are generally used for asset protection and are usually tax neutral. Their ultimate function is to provide for the beneficiaries. Some proponents advertise APTs as allowing foreign trustees to ignore U.S. court orders and to simply transfer the trust to another jurisdiction in response to legal action threatening the trust's assets.

Payments to the beneficiaries of a trust can also be used in the money laundering process, because these payments do not have to be justified as compensation or as a transfer of assets for services rendered.

Lawyers often serve as trustees by holding money or assets “in trust” for clients. This enables lawyers to conduct transactions and to administer the affairs of a client. Sometimes, the illicit money is placed in a law firm's general trust account in a file set up in the name of the client, a nominee or a company controlled by the client. Also, trust accounts are used as part of the normal course of a lawyer's duties in collecting and disbursing payments for real property on behalf of clients.

---

## Terrorist Financing

---

After the terrorist attacks of September 11, 2001, the finance ministers of the Group of Seven (G-7) met on October 7, 2001, in Washington, D.C., and urged all nations to freeze the assets of known terrorists. Since then, many countries have committed themselves to helping disrupt terrorist assets by alerting financial institutions about persons and organizations that authorities determine are linked to terrorism. The G-7 nations marshaled FATF to hold an “extraordinary plenary session”

on October 29, 2001, in Washington to address terrorist financing. As a result, FATF issued the first eight of its Special Recommendations, which have since been incorporated into the current FATF Recommendations. (*See Chapter 2 for more detail.*)

Recommendation 5 encourages countries to criminalize terrorist financing and the financing of terrorist organizations and individual terrorists with or without a link to a specific terrorist act, as well as ensuring these crimes are designated as money laundering predicate offenses. This allows the application of money laundering statutes to terrorist financing and the potential for greater prosecution and deterrence. Cutting off financial support to terrorists and terrorist organizations is essential to disrupting their operations and preventing attacks.

## **DIFFERENCES AND SIMILARITIES BETWEEN TERRORIST FINANCING AND MONEY LAUNDERING**

Money laundering and terrorist financing are often mentioned in the same breath, without much consideration to the critically important differences between the two. Many of the controls that businesses should implement are meant to serve the dual purposes of combating both money laundering and terrorist financing. The U.S. 2015 Terrorist Financing Risk Assessment noted that controls instituted to combat money laundering have also strengthened our ability to identify, deter and disrupt terrorist financing. Of the individuals investigated by law enforcement for ties to terrorist organizations who had associated BSA records, 58 percent were reported as having engaged in suspected money laundering, including structuring.

But the two are separate crimes, and, although no one has been able to create a workable financial profile for operational terrorists, there are key distinctions that can help compliance officers understand the differences and can help distinguish suspicious terrorist financial activity from money laundering.

The most basic difference between terrorist financing and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. The purpose of laundering funds intended for terrorists is to support terrorist activities. The individuals responsible for raising the funds are not the beneficiaries of the laundered funds. The money benefits terrorist activity. On the other hand, money laundering always involves the proceeds of illegal activity. The purpose of laundering is to enable the money to be used legally. The individuals responsible for the illegal activity are usually the ultimate beneficiaries of the laundered funds.

From a technical perspective, the laundering methods used by terrorists and other criminal organizations are similar. Although it would seem logical that funding from legitimate sources does not need to be laundered, there is a need for the terrorist group to disguise the link between it and its legitimate funding sources, one reason being the continued and uncompromised future use of that source. In doing so, the terrorists use methods similar to those of criminal organizations: cash smuggling, structuring, purchase of monetary instruments, wire transfers and use of debit, credit and/or prepaid cards. The hawala system, an informal value transfer system involving the international transfer of value outside the legitimate banking system and based on a trusted network of individuals, has also played a role in moving terrorist-related funds. In addition, money raised for terrorist groups is also used for mundane expenses, such as food and rent, and is not always strictly used for just the terrorist acts themselves.

## DETECTING TERRORIST FINANCING

In its 2004 *Monograph on Terrorist Financing*, the National Commission on Terrorist Attacks Upon the United States stated that neither the September 11 hijackers nor their financial facilitators were experts in the use of the international financial system. The terrorists created a paper trail linking them to each other and their facilitators. Still, they were adept enough to blend into the vast international financial system without revealing themselves as criminals. The money laundering controls in place at the time were largely focused on drug trafficking and large-scale financial fraud and were not sufficiently focused on the transactions engaged in by the hijackers. Since 9/11, international efforts to detect and deter terrorist financing have increased significantly. Conversely, in response to these efforts, terrorists and terrorist financiers have adapted, expanding and varying their methods of raising and moving funds, requiring increased innovation and vigilance by law enforcement and financial institutions.

### Case Study

The September 11 hijackers used U.S. and foreign financial institutions to hold, move and retrieve their money. They deposited money into U.S. accounts, primarily by wire transfers and deposits of cash or traveler's checks brought from overseas. Several of them kept funds in foreign accounts that they accessed in the United States through ATM and credit card transactions. The hijackers received funds from facilitators in Germany and the United Arab Emirates as they transited Pakistan before coming to the United States. The plot cost al Qaeda somewhere in the range of \$400,000–\$500,000, of which approximately \$300,000 passed through the hijackers' bank accounts in the United States. While in the United States, the hijackers spent money primarily for flight training, travel and living expenses.

Through reconstruction of available financial information, the U.S. Internal Revenue Service and the U.S. Federal Bureau of Investigation established how the hijackers responsible for the September 11 attacks received their money and how the money was moved into and out of their accounts. The 19 hijackers opened 24 domestic bank accounts at four different banks. The following financial profiles were developed from the hijackers' domestic accounts.

### Account Profiles

- Accounts were opened with cash or cash equivalents in average amounts of \$3,000 to \$5,000.
- Identification used to open the accounts were visas issued through foreign governments.
- Accounts were opened within 30 days after entry into the United States.
- Some of the accounts were joint accounts.
- Addresses used usually were not permanent addresses but rather were mailboxes and were changed frequently.
- The hijackers often used the same address and telephone numbers on the accounts.
- Twelve hijackers opened accounts at the same bank.

### Transaction profiles

- Some accounts directly received and sent wire transfers of small amounts to and from foreign countries, such as United Arab Emirates (UAE), Saudi Arabia and Germany.
- The hijackers made numerous attempts to withdraw cash in excess of the limit of the debit card.
- Numerous balance inquiries were made.
- After a deposit was made, withdrawals occurred immediately.
- Overall transactions were below reporting requirements.
- Funding of the accounts was by cash and overseas wire transfers.
- ATM transactions occurred with more than one hijacker present (creating a series of transactions involving several hijackers at the same ATM).
- Debit cards were used by hijackers who did not own the accounts.

### International activity

- While in the United States, two of the hijackers had deposits made on their behalf by unknown individuals.
- Hijackers on all four flights purchased traveler's checks overseas and brought them into the United States. Some of these traveler's checks were deposited into their U.S. checking accounts.
- One of the hijackers received substantial funding through wire transfers into his German bank account in 1998 and 1999 from an individual.
- In 1999, this same hijacker opened an account in UAE, giving a power of attorney over the account to the same individual who had been wiring money to his German account.
- More than \$100,000 was wired from the UAE account of the hijacker to the German account of the same hijacker in a 15-month period.

In an attempt to clarify terrorist financing and offer recommendations to the global financial community, FATF has issued guidance to identify techniques and mechanisms used in financing terrorism. The report, entitled *Guidance for Financial Institutions in Detecting Terrorist Financing*, was published on April 24, 2002, and described the general characteristics of terrorist financing. Its objective was to help financial institutions determine whether a transaction merits additional scrutiny so that the institution is better able to identify, report (when appropriate) and ultimately avoid transactions involving the funds associated with terrorist activity. In the report, FATF suggested that financial institutions exercise "reasonable judgment" in evaluating potential suspicious activity. To avoid becoming conduits for terrorist financing, institutions must look at, among other things, the following factors.

- Use of an account as a front for a person with suspected terrorist links
- Appearance of an account holder's name on a list of suspected terrorists
- Frequent large cash deposits in accounts of nonprofit organizations
- High volume of transactions in the account

- Lack of a clear relationship between the banking activity and the nature of the account holder's business

FATF suggested that, with these scenarios in mind, financial institutions pay attention to some classic indicators of money laundering, including dormant, low-sum accounts that suddenly receive wire transfer deposits followed by daily cash withdrawals that continue until the transferred sum is removed and lack of cooperation by the client in providing required information.

## HOW TERRORISTS RAISE, MOVE AND STORE FUNDS

Global sanctions efforts have reduced funding to organizations from traditional state sponsors of terror, leading those organizations to seek supplemental sources of income to conduct their activities.

In a December 2015 United Nations Security Council meeting, Secretary-General Ban Ki-moon told the Council, "Terrorists take advantage of weaknesses in financial and regulatory regimes to raise funds. They circumvent formal channels to avoid detection and exploit new technologies and tools to transfer resources. They have forged destructive and very profitable links with drug and criminal syndicates—among others. And they abuse charitable causes to trick individuals to contribute. Terrorists continue to adapt their tactics and diversify their funding sources," which he noted include raising money through the oil trade, extortion, undetected cash couriers, kidnapping for ransom, trafficking of humans and arms and racketeering.

## Use of Hawala and Other Informal Value Transfer Systems

Alternative remittance systems (ARSs) or informal value transfer systems (IVTSs) are often associated with ethnic groups from Africa, Asia and the Middle East. ARSs commonly involve the international transfer of value outside the legitimate banking system and are based on trust. The systems are referred to by different names depending upon the country: "hawala" (an Arabic word meaning change or transform), "hundi" (a Hindi word meaning collect), "chiti banking" (referring to the way the system operates), "chop shop banking" (China) and "poey kuan" (Thailand).

Hawala was created centuries ago in India and China before Western financial systems were established to facilitate the secure and convenient movement of funds. Merchant traders wishing to send funds to their homelands would deposit them with a hawala broker or hawaladar who normally owned a trading business. For a small fee, the hawaladar would arrange for the funds to be made available for withdrawal from another hawaladar, normally also a trader, in another country. The two hawaladars would settle accounts through the normal process of trade.

Today, the process works much the same way, with people in various parts of the world using their accounts to move money internationally for third parties. In this way, deposits and withdrawals are made through hawala bankers rather than traditional financial institutions. The third parties are normally immigrants or visiting workers who send small sums to their homelands to avoid bank fees for wire transfers. Reasons for legitimate use of hawala and other IVTS include cheaper and faster money transmission, lack of banking access in the remittance-receiving country, cultural preference and lack of trust in the formal banking system. There is usually no physical movement of currency and a lack of formality with regard to verification and record-keeping. The money transfer

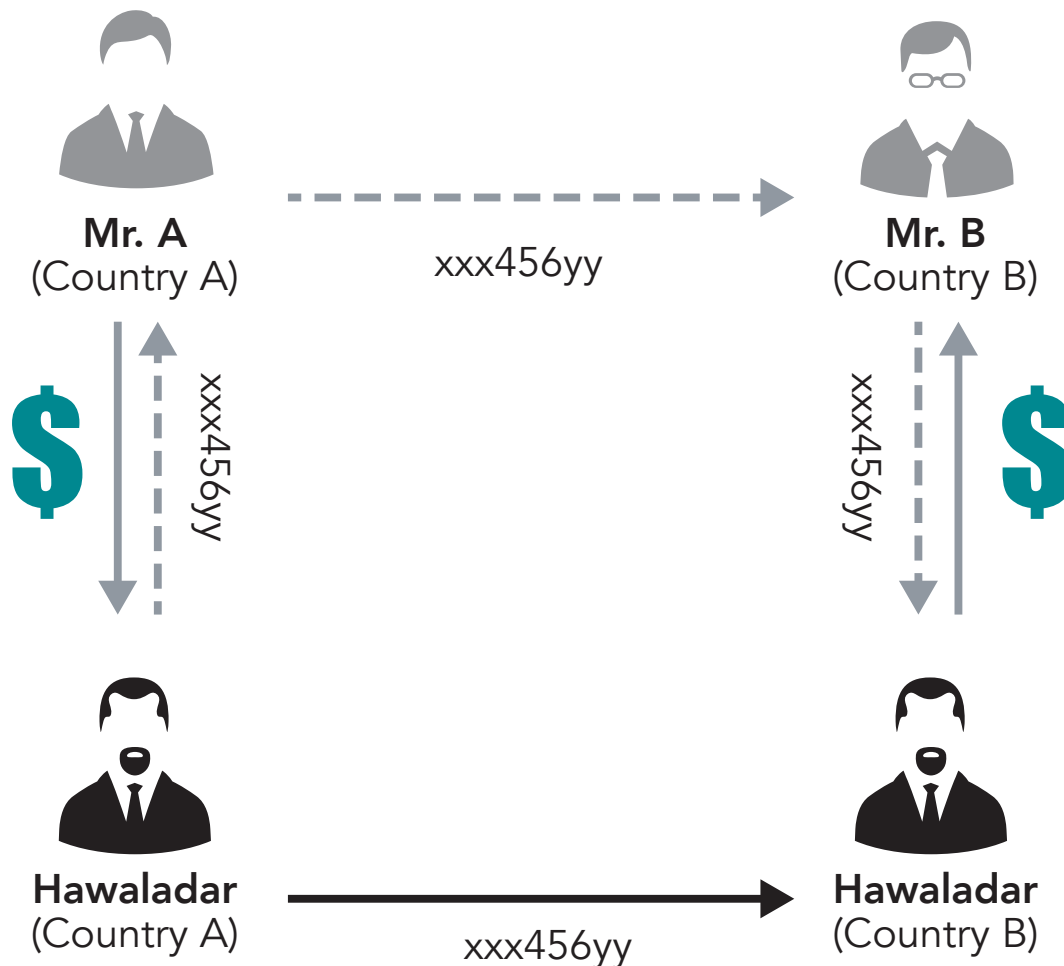
takes place by coded information that is passed through chits, couriers, letters, faxes, emails, text messages or online chat systems, followed by some form of telecommunications confirmation. Almost any document that carries an identifiable number can be used by the receiver to pick up the values in the other country.

As anti-money laundering measures have proliferated around the world, the use of hawala, which operates without governmental supervision, is believed to have become more appealing to money launderers and terrorists. In its 2013 report *The Role Of Hawala And Other Similar Service Providers In ML/TF*, FATF explains that regulation and supervision of hawalas and other similar service providers remains a key challenge to authorities, also noting that as in other sectors, money laundering and terrorist financing risk increases the less regulation and supervision the hawala or similar service provider is subjected to. It is attractive for launderers because it leaves little to no paper trail because the details of the customers who will receive the funds are communicated to the receiving brokers via telephone, fax and email. Recently, authorities have been observing the use of advanced Internet technologies by hawala and other similar agents and suspect they are exclusively using protected online services to conduct their activities and maintain their accounts, leaving no manual accounts.

Because hawala is a remittance system, it can be used at any phase of the money laundering cycle. It can provide an effective means of placement: when the hawaladar receives cash, he can deposit the cash in bank accounts. He will justify these deposits to bank officials as the proceeds of legitimate business. He may also use some of the cash received to pay for his business expenses, reducing his need to deposit the cash into the bank account. Hawaladars often operate within or in addition to a legitimate or front business to provide cover for the activity and commingle the funds in the business accounts.

A component of many layering schemes is transferring money from one account to another, while trying not to leave a paper trail. A basic hawala transfer leaves little if any paper trail. Hawala transfers can be layered to make following the money even more difficult. This can be done by using hawaladars in several countries and by distributing the transfers over time.

## Hawala Transaction Example



Hawala techniques can be used to transform money into almost any form, offering many possibilities for establishing an appearance of legitimacy in the integration phase of the money laundering cycle. The money can be reinvested in a legitimate (or legitimate appearing) business. The hawaladar can very easily arrange for the transfer of money from the United States to Pakistan and then back to the United States, apparently as part of an investment in a business there.

Hawalas are attractive to terrorist financiers because they, unlike formal financial institutions, are not consistently subject to formal government oversight and are not required to keep detailed records in a standard form. Although some hawaladars do keep ledgers, their records are often written in idiosyncratic shorthand and are maintained only briefly. Al Qaeda moved much of its money by hawala before September 11, 2001. Al Qaeda used about a dozen trusted hawaladars who almost certainly knew of the source and purpose of the money. Al Qaeda also used unwitting hawaladars who probably strongly suspected that they were dealing with al Qaeda but were nevertheless willing to engage in the transactions.

### Case Study

On August 18, 2011, Mohammad Younis pled guilty in Manhattan federal court to operating an unlicensed money transfer business between the United States and Pakistan. One of the money transfers was used to fund the May 1, 2010, attempted car bombing in New York City's Times Square by Faisal Shahzad, who is serving a life sentence in federal prison. From January to May 2010, Younis provided money transmitting services to individuals in the New York City area by assisting in the operation of a hawala. On April 10, 2010, Younis engaged in two separate hawala transactions with customers who traveled from Connecticut and New Jersey to meet with him in Long Island. In each of the transactions, Younis provided thousands of dollars in cash to the individuals at the direction of a coconspirator in Pakistan but without knowledge of how the customers were planning to use the funds. At no time did Younis have the license to operate a money transmitting business from either state or federal authorities. One of the individuals to whom Younis provided money was Shahzad, who on June 21, 2010, pled guilty to a 10-count indictment charging him with crimes relating to his attempt to detonate a car bomb in Times Square on May 1, 2010. During the course of his plea allocution, Shahzad acknowledged receiving a cash payment in April 2010 in the United States to fund his preparations for the May 1, 2010, attempted bombing. According to Shahzad, the April cash payment was arranged in Pakistan by associates of the Tehrik-e-Taliban, the militant extremist group based in Pakistan that trained him to make and use explosive devices. On September 15, 2010, Younis was arrested by the FBI and other agents of the New York Joint Terrorism Task Force. Younis pled guilty to one count of conducting an unlicensed money transmitting business.

## **Use of Charities or Nonprofit Organizations (NPOs)**

---

After the September 11, 2001, attacks the U.S. government initiated the Terrorist Finance Tracking Program (TFTP) in order to identify, track and pursue terrorist groups' sources of funding. Through the TFTP, the U.S. government has uncovered and shut down over 40 designated charities used as potential fundraising front organizations.

Knowingly or not, charitable organizations have served as vehicles for raising and laundering funds destined for terrorism. As a result, some charities, particularly those with Muslim connections, have seen a large drop in donations or have become targets of what they claim are unfair investigations or accusations. FATF states in its 2014 *Risk of Terrorist Abuse in Non-Profit Organizations* (NPO): "The importance of the NPO sector to the global community cannot be overstated. It is a vibrant sector, providing innumerable services to millions of people." However, this typologies project found that more than a decade after the abuse of NPOs by terrorists and terrorist organizations was formally recognized as a concern, the terrorism threat to the sector remains, and the sector continues to be misused and exploited by terrorist organizations through a variety of means.

Charities or nonprofit organizations have the following characteristics that are particularly vulnerable to misuse for terrorist financing.

- Enjoying the public trust
- Having access to considerable sources of funds

- Being cash-intensive
- Frequently having a global presence, often in or next to areas exposed to terrorist activity
- Often being subject to little or no regulation and/or having few obstacles to their creation

To help legitimate NPOs avoid ties to terrorist-related entities and to help them regain public trust, FATF first issued guidelines in 2002 on best practices for charities in combating the abuse of non-profit organizations. The best practices guidance was updated in 2015 with the purpose of helping countries implement Recommendation 8 on NPOs in line with the risk-based approach: to assist NPOs in mitigating terrorist-financing threats and assisting financial institutions in the proper implementation of the risk-based approach when providing financial services to NPOs.

The objective of Recommendation 8 is to ensure that NPOs are not abused by

- terrorist organizations posing as legitimate entities;
- exploiting legitimate entities as conduits for terrorist financing; and
- concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

The best practices cover identification and mitigation of risk by countries and NPOs alike, self-regulation by NPOs and their access to financial services. FATF recommends that NPOs

- maintain and be able to present full program budgets that account for all expenses; and
- conduct independent internal audits and external field audits, the latter to ensure funds are being used for intended purposes.

FATF recommends that charities use formal bank accounts to store and transfer funds so that they are subject to the banks' regulations and controls. In turn, the banks where the accounts are established can treat NPOs like other customers, apply their know-your-customer rules and report suspicious activities.

The Charity Commission is an independent regulator of charities in England and Wales whose role is to protect the public's interest in charities and ensure that charities further their charitable purposes for the public benefit and remain independent from private, government or political interests. Its *Counter-Terrorism Strategy* report dictates a four-strand approach to preventing abuse of charities by terrorist financiers.

- Cooperation with government regulators and law enforcement nationally and internationally
- Raising awareness in the sector of the risks charities face from terrorism
- Oversight and supervision through proactive monitoring of the sector in areas identified as being at higher risk
- Intervention when abuse, or the risk of abuse, related to terrorist activity is apparent

### Case Study

In May 2013, two U.S. women from Minnesota were sentenced in federal court for providing material support to a U.S.-designated terrorist organization, al-Shabaab. Amina Farah Ali and Hawo Mohamed Hassan, naturalized U.S. citizens from Somalia, were sentenced to 240 and 120 months, respectively, in federal prison for charges ranging from making false statements to authorities to providing material support to a terrorist organization. Evidence presented at trial proved the defendants provided support to al-Shabaab from September 2008 through July 2009. After communicating with Somalia-based members of al-Shabaab requesting financial assistance on behalf of the group, the women, along with the help of others, raised money for the terrorist organization by soliciting funds in Somali neighborhoods in Minnesota and other cities in the United States and Canada. Funds were often sought under false pretenses, leading those who donated to believe they were helping the less fortunate. Funds in direct support of al-Shabaab were obtained by the defendants through participation in teleconferences that featured speakers who encouraged listeners to make donations. Once they received the funds, Ali and others utilized multiple remittance services for in excess of 12 fund transfers using false recipient names to conceal the true intended beneficiary, al-Shabaab.

### Case Study

The Holy Land Foundation (HLF) was an Islamic charitable organization operating multiple locations in the United States and based out of Richardson, Texas. HLF was shut down by the U.S. Treasury in 2001 and designated for its support of U.S.-designated foreign terrorist organization, Hamas. This support consisted of direct fund transfers to HLF offices in the West Bank and Gaza affiliated with Hamas and transfers of funds to Islamic charity committees and other charitable organizations that are part of Hamas or controlled by its members. HLF and five of its leaders were convicted in November 2008 by the U.S. government on charges of providing material support for terrorism. A similar organization, International Relief Fund for the Afflicted and Needy-Canada (IRFAN-Canada), was identified and declared a terrorist entity in April 2014 by Public Safety Canada under the Criminal Code. The Canadian government alleged that, between 2005 and 2009, the group funneled \$14.6 million to Hamas. It has also been alleged that those funds originated in part from HLF and were subsequently transferred to a UK-based nonprofit organization, which in turn routed the funds to several Palestinian aid organizations in Gaza and the West Bank known to be under the control of Hamas or its leaders. Both HLF and IRFAN-Canada are believed to have been created solely for the purpose of raising support, financial and otherwise, for Hamas.

---

## Emerging Risks for Terrorist Financing

---

The FATF's 2015 *Emerging Terrorist Financing Risks* details rising threats as the following.

- **Self-funding by FTFs**

The advent of social media, smartphone applications and Internet sharing sites now provide terrorist organizations global reach at little to no cost. Foreign terrorist fighters (FTFs) and terrorist sympathizers can self-radicalize and/or communicate with terrorist organizations like never before. The often low cost associated with perpetrating a terrorist act on a soft target

(i.e., a civilian, nonmilitary target that is relatively unprotected and thus vulnerable to terrorist attacks) means such acts can be self-funded. Self-funding includes sources such as employment income, social assistance, family support and bank loans, which makes detection nearly impossible without the association of other aggravating terrorist financing indicators.

Former FBI Director James Comey stated at a U.S. Senate Judiciary Hearing on December 9, 2015, “Terrorists, in ungoverned spaces, disseminate poisonous propaganda and training materials to attract troubled souls around the world to their cause. They encourage these individuals to travel, but if they cannot travel, they motivate them to act at home. This is a significant change from a decade ago.”

### Case Study

On December 2, 2015, in San Bernardino, California, Syed Rizwan Farook and his wife, Tashfeen Malik, opened fire on his coworkers at a party, killing 14 people and injuring 22. The couple was subsequently killed during a shootout with police. Federal authorities have said Farook spent years becoming more radicalized and violence-oriented, in part by watching videos that advocated jihad. On the day of the attack, a Facebook account used by his wife posted a pledge of allegiance to the terror group ISIS (Islamic State in Iraq and Syria). This attack was consistent with the profile for many terrorist acts in that it appears to have required a low total dollar amount to carry out. Farook was employed by the State of California as a health inspector, providing him a source of income with which to obtain some of the weapons used in the commission of the act (a straw purchaser was used to obtain the weapons). He received additional funding through a \$28,500 loan provided by an online peer-to-peer lender that matches investors with borrowers. No specific indicators were identified that would have alerted the lender to the shooter’s intentions and by all accounts his employment profile and creditworthiness provided sufficient reason to complete the loan.

- **Raising funds through the use of social media**

Social media has created the ability to build social and information-sharing networks like never before in human history. This incredible advance in technology presents a unique opportunity for terrorist organizations to communicate and raise money for their causes and the potential to reach into every home in every country in near real time. Crowdfunding and sharing of virtual or prepaid account information are a few of the methods through which social media has been leveraged by terrorists. This presents unique difficulties for law enforcement not only due to the increased dispersion of the activity but also the need for cooperation from both financial institutions and social media platforms.

### Case Study

An example of an individual raising funds through social media is Shafi Sultan Mohammad al-Ajmi, designated by the U.S. Treasury in August 2014 as a supporter of terrorists in Syria and Iraq. Al-Ajmi operates regular social media campaigns seeking donations for Syrian fighters and is one of the most active Kuwaiti fundraisers for Al Nusra Front (ANF). Al-Ajmi publicly admitted that he collected money under the auspices of charity and delivered the funds in person to ANF and acknowledged purchasing and smuggling arms on behalf of ANF.

- **New payment products and services** (*See Risks Associated with New Payment Products and Services*)
- **Exploitation of natural resources**

Terrorist organizations that hold or maintain control over territory or operate in a country with poor governmental control of the territory may take control of natural resources, such as gas, oil, timber, diamonds, gold (and other precious metals), wildlife (e.g., ivory trading) and historical artifacts or extort companies that extract those resources to both fund terrorist acts and support day-to-day activities. These resources themselves may be sold on the black market or to complicit companies where they can then be integrated into the global trade sector. An awareness of geographies where terrorist organizations operate or maintain control, current commodity prices and strong multi-jurisdictional partnerships are necessary to combat this method of terrorist funding, which has the potential to generate vast sums.

**NOTES:**

[illegible]

[illegible]

[illegible]

# Chapter 2

## International AML/CFT Standards

### Financial Action Task Force (FATF)

---

**T**he pace of international activity in the anti-money laundering (AML) field accelerated in 1989 when the Group of Seven nations launched the Financial Action Task Force (FATF) at its annual economic summit in Paris. With France serving as its first chair, this multinational group started working toward a coordinated effort against international money laundering.

Originally referred to as the G-7 Financial Action Task Force, today FATF serves as the vanguard in promulgating AML guidance to governmental bodies around the globe. The International Monetary Fund (IMF) and the World Bank also offer important perspectives to the field.

FATF has brought significant changes to the ways that banks and businesses around the world conduct their affairs. It also has brought about changes in laws and in governmental operations.

The intergovernmental body is based at the Organization for Economic Cooperation and Development (OECD) in Paris, where it has its own secretariat. FATF can be located online at <http://www.fatf-gafi.org/>.

### FATF Objectives

---

FATF's stated objectives are to "set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Starting with its own members, the FATF monitors countries' progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and counter-measures; and, promotes the adoption and implementation of the FATF Recommendations globally."

FATF fulfills these objectives by focusing on several important tasks, which include the following.

1. Spreading the AML message worldwide: The group promotes the establishment of a global AML and anti-terrorist financing network based on expansion of its membership, the development of regional AML bodies in various parts of the world and cooperation with other international organizations.

## 2. Monitoring implementation of the FATF Recommendations among its members.

In 2011, FATF concluded its third round of mutual evaluations of all its members. The process began in 2004. For its fourth round of mutual evaluations, which started in 2014, it adopted a new approach for assessing technical compliance with the Recommendations and assessing if a member's AML/CFT system is effective.

The new Methodology, which was released in 2013, is informed by the experience of FATF, FATF-style regional bodies (FSRBs), the International Monetary Fund (IMF) and the World Bank in conducting assessments of compliance with earlier versions of the FATF Recommendations. Collectively, the technical compliance and effectiveness assessments provide an integrated analysis of the extent to which the country is compliant with the FATF Recommendations and how successful it is in maintaining a strong AML/CFT system. It focuses on the following.

- **Technical Compliance Assessment:** Evaluates the specific requirements of the FATF Recommendations, including how a member relates them to its relevant legal and institutional framework, and the powers and procedures of its competent authorities. The focus is on the fundamental building blocks of an AML/CFT system.

For each Recommendation, assessors reach a conclusion about whether a country complies with the FATF standard. The result is a rating of five possible levels of technical compliance.

- Compliant
  - Largely compliant
  - Partially compliant
  - Noncompliant
  - Not applicable
- **Effectiveness Assessment:** Seeks to assess the adequacy of a member's implementation of the FATF Recommendations and identifies the extent to which a member achieves a defined set of outcomes that are central to a robust AML/CFT system. The focus is on the extent to which the legal and institutional framework of the member is producing the expected results.

For the purposes of the 2013 Methodology, FATF defines effectiveness as "the extent to which the defined outcomes are achieved." Effectiveness is evaluated on the basis of 11 Immediate Outcomes.

1. Money laundering/terrorist financing (ML/TF) risks are known and actions coordinated to combat or thwart the proliferation of ML/TF.
2. International cooperation provides actionable information to use against criminals.
3. Supervisors regulate financial institutions and nonbank financial institutions (NBFIs) and their risk-based AML/CFT programs.
4. Financial institutions and NBFIs apply preventative measures and report suspicious transactions.

5. Legal persons are not misused for ML/TF and beneficial ownership information is available to authorities.
6. Financial intelligence information is used by authorities in money laundering and terrorist financing investigations.
7. Money laundering offenses are investigated and criminally prosecuted, and sanctions are imposed.
8. Proceeds of crime are confiscated.
9. Terrorist financing offenses are investigated and criminally prosecuted, and sanctions are imposed.
10. Terrorists and terrorist organizations are prevented from raising, moving and using money and are not permitted to abuse nonprofit organizations (NPOs).
11. Persons and organizations involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using money.

Each of the 11 Immediate Outcomes represents a key goal of an effective AML/CFT system. They also feed into the three Intermediate Outcomes that represent major thematic goals of AML/CFT measures.

1. Policy, cooperation and coordination to mitigate money laundering and terrorist financing.
2. Prevention of proceeds of crime entering into the financial system and reporting of such when they do.
3. Detection and disruption of ML/TF threats. For each individual Immediate Outcome, assessors reach conclusions about the extent to which a country is (or is not) effective and provide an effectiveness rating based on the extent to which the core issues and characteristics are addressed.
  - High level of effectiveness
  - Substantial level of effectiveness
  - Moderate level of effectiveness
  - Low level of effectiveness

If a country has not reached a high level of effectiveness, then assessors give reasons why it fell below the standard and recommend measures the country should take to improve its ability to achieve the outcome.

FATF does not have the power to impose fines or penalties against recalcitrant member-nations. However, in 1996, FATF launched a policy for dealing with nations that fail to comply with the FATF Recommendations that it describes as “a graduated approach aimed at enhancing peer pressure.” This graduated approach ranges from requiring the country to deliver a progress report at plenary meetings to suspension of membership.

In September 1996, Turkey became the first FATF member exposed to the peer pressure policy. Although a member since 1990, Turkey had yet to criminalize money laundering. FATF issued a warning to financial institutions worldwide to be vigilant of business relations and transactions with people and entities in Turkey due to its lack of laundering controls. One month later, Turkey enacted a money laundering law.

### 3. Reviewing money laundering trends and countermeasures.

Faced with a financial system that has few geographic limitations, operates around the clock in every time zone and maintains the pace of the global electronic highway, criminals are constantly searching for new points of vulnerability and adjusting their laundering techniques to respond to countermeasures introduced by FATF members and other countries. As such, FATF members are continually gathering information on money laundering trends to ensure the organization's Recommendations remain up to date. For example, in October 2013, FATF and the Egmont Group of Financial Intelligence Units released a research report titled *Money Laundering And Terrorist Financing Through Trade In Diamonds*, which examined the vulnerabilities and risks of the "diamond pipeline" and covered all sectors of the diamond trade, including production, rough diamond sale, cutting and polishing, jewelry manufacturing and jewelry retailers.

Since its creation in 1989, FATF has been working under 5-year mandates. In May 2004, its members extended the organization's charter by a record 8 years, signaling the possibility that it may become a permanent institution in global money laundering and terrorist financing control efforts. In April 2012, the mandate was extended to December 31, 2020.

Since its establishment, FATF has focused its work on three main activities: (1) standard setting, (2) ensuring effective compliance with the standards, (3) and identifying money laundering and terrorist financing threats.

These activities will remain at the core of FATF's work for the remainder of the mandate. Going forward, FATF will build on the work and respond to new and emerging threats, such as proliferation financing and vulnerabilities in new technologies that could destabilize the international financial system.

## FATF 40 Recommendations

---

A key element of FATF's efforts is its detailed list of appropriate standards for countries to implement. These measures are set out in the 40 Recommendations, which were first issued in 1990 and revised in 1996, 2003 and 2012. FATF has also issued various Interpretative Notes designed to clarify the application of specific Recommendations and to provide additional guidance.

After the events of September 11, 2001, FATF adopted and published the *FATF IX Special Recommendations* on terrorist financing. The first eight Special Recommendations were adopted on October 31, 2001, and the ninth on October 22, 2004. The 2012 revisions combined the IX Special Recommendations into the 40 Recommendations.

FATF's Recommendations have become the world's blueprint for effective national and international AML- and CFT-related controls. The IMF and the World Bank have recognized the FATF Recommendations as the international standard for combating money laundering and terrorist financing. In 2002, the IMF, the World Bank and FATF agreed to a common methodology to assess compliance with the FATF Recommendations.

The 40 Recommendations provide a complete set of countermeasures against money laundering and terrorist financing, covering

- the identification of risks and development of appropriate policies;
- the criminal justice system and law enforcement;
- the financial system and its regulation;
- the transparency of legal persons and arrangements; and
- international cooperation.

FATF recognizes that because countries have different legal and financial systems, they cannot use identical measures to fight money laundering and terrorist financing. The Recommendations set minimum standards of action for countries to implement according to their particular circumstances and constitutional frameworks. With its 2012 revision, FATF introduced the risk assessment as the first recommendation, underscoring that assessing risk is the first step in combating money laundering and terrorist financing.

With its 2003 revisions of the 40 Recommendations, the FATF expanded the reach of its global blueprint for cracking down on illicit movements of funds. It introduced substantial changes intended to strengthen measures to combat money laundering and terrorist financing, which established further enhanced standards by which countries can better combat money laundering and terrorist financing.

The most important changes made to the Recommendations in 2003 were as follows.

- Expanded coverage to include terrorist financing
- Widened the categories of business that should be covered by national laws, including real estate agents, precious metals dealers, accountants, lawyers and trust services providers
- Specified compliance procedures on issues such as customer identification and due diligence, including enhanced identification measures for higher risk customers and transactions
- Adopted a clearer definition of money laundering predicate offenses
- Encouraged prohibition of so-called shell banks, typically set up in offshore secrecy havens and consisting of little more than nameplates and mailboxes, and urged improved transparency of legal persons and arrangements
- Included stronger safeguards, notably regarding international cooperation in, for example, terrorist financing investigations

In 2012, the Recommendations were revised again, incorporating the IX Special Recommendations on terrorist financing into the 40 Recommendations. The most important changes in this revision were

- creation of a Recommendation on assessing risks and applying a risk-based approach to all AML/CFT efforts;
- creation of a Recommendation for targeted financial sanctions related to the proliferation of weapons of mass destruction;
- more attention on domestic politically exposed persons (PEPs) and those entrusted with a prominent function by an international organization;
- new requirement for the identification and assessment of risks of new products prior to the launch of the new product;
- new requirement for financial groups to implement group-wide AML/CFT programs and have procedures for sharing information within the group; and
- inclusion of tax crimes within the scope of designated categories of offenses for money laundering.

Group	Topic	Recommendations
I	<b>AML/CFT Policies and Coordination</b> <ul style="list-style-type: none"> <li>• Assessing risks and applying a risk-based approach</li> <li>• National cooperation and coordination</li> </ul>	1–2
II	<b>Money Laundering and Confiscation</b> <ul style="list-style-type: none"> <li>• Money laundering offenses</li> <li>• Confiscation and provisional measures</li> </ul>	3–4
III	<b>Terrorist Financing and Financing of Proliferation</b> <ul style="list-style-type: none"> <li>• Terrorist financing offenses</li> <li>• Targeted financial sanctions related to terrorism and terrorist financing</li> <li>• Targeted financial sanctions related to proliferation</li> <li>• Nonprofit organizations</li> </ul>	5–8
IV	<b>Financial and Nonfinancial Institution Preventative Measures</b> <ul style="list-style-type: none"> <li>• Financial institution secrecy laws</li> <li>• Customer due diligence and record-keeping</li> <li>• Additional measures for specific customers and activities</li> <li>• Reliance, controls and financial groups</li> <li>• Reporting of suspicious transactions</li> <li>• Designated nonfinancial businesses and professions</li> </ul>	9–23

Group	Topic	Recommendations
V	<b>Transparency and Beneficial Ownership of Legal Persons and Arrangements</b> <ul style="list-style-type: none"> <li>• Transparency and beneficial ownership of legal persons</li> <li>• Transparency and beneficial ownership of legal arrangements</li> </ul>	24–25
VI	<b>Powers and Responsibilities of Competent Authorities and Other Institutional Measures</b> <ul style="list-style-type: none"> <li>• Regulation and supervision</li> <li>• Operational and law enforcement</li> <li>• General requirements</li> <li>• Sanctions</li> </ul>	26–35
VII	<b>International Cooperation</b> <ul style="list-style-type: none"> <li>• International instruments</li> <li>• Mutual legal assistance</li> <li>• Mutual legal assistance regarding freezing and confiscation</li> <li>• Extradition</li> <li>• Other forms of international cooperation</li> </ul>	36–40

Some highlights of the 2012 revision of the 40 Recommendations are as follows.

- **Risk-based approach:** Countries should start by identifying, assessing and understanding the money laundering and terrorist financing risks they face. Then they should take appropriate measures to mitigate the identified risks. The risk-based approach allows countries to allocate their limited resources in a targeted manner in line with their own particular circumstances in order to increase the efficiency of preventative measures. Financial institutions should also use the risk-based approach to identify and mitigate the risks they face.
- **Designated categories of offenses:** The Recommendations specify crimes, called “designated categories of offenses,” that should serve as money laundering predicates (i.e. crimes that offenders attempt to conceal through financial subterfuge that should constitute precursory offenses to money laundering). Countries should also put in place provisions to allow for the confiscation of the proceeds of crime or otherwise prevent criminals from having access to their criminal proceeds.
- **Terrorist financing and financing of proliferation:** Countries should criminalize terrorist financing, including the financing of terrorist acts, organizations and individual terrorists, even if no terrorist activity can be directly attributed to the provision of financing. Countries should impose sanction regimes that will allow them to freeze the assets of persons designated by the United Nations Security Council for involvement in terrorism or the proliferation of weapons of mass destruction. Countries should also establish sufficient controls to mitigate the misuse of nonprofit organizations to provide support to terrorists.
- **Knowledge and criminal liability:** The Recommendations include the concept that knowledge required for the offense of money laundering may be inferred from objective factual circumstances. This is similar to what is known in some countries as “willful blindness,” or deliberate avoidance of knowledge of the facts. In addition, the Recommendations urge that criminal liability—or civil or administrative liability, where criminal liability is not possible—should apply to legal persons as well.

- **Customer due diligence (CDD) measures:** Financial institutions should conduct customer due diligence when they
  - establish business relations;
  - carry out an occasional transaction or a wire transfer above the specified threshold;
  - have a suspicion of money laundering or terrorist financing; and
  - have doubts about the veracity or adequacy of previously obtained customer identification information.

Financial institutions must, using a risk-based approach

- identify the customer and verify that customer's identity using reliable, independent source documents, data or information. Establishing accounts in anonymous or obviously fictitious names should be prohibited;
  - take reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include understanding the ownership and control structure of the customer;
  - understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship;
  - conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken in the course of that relationship to ensure that the transactions are consistent with the institution's knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds;
  - maintain records of the above customer information as well as all transactions to enable them to comply with requests from competent authorities;
  - rely on other parties to conduct customer due diligence in certain circumstances; however, the relying institution remains liable for compliance with completing the required customer due diligence; and
  - establish group-wide AML program for financial groups.
- **Additional customer due diligence on specific customers and activities:** Some customer types and activities pose heightened risks, especially the following.
    - **Politically exposed persons (PEPs):** Appropriate steps must be taken to identify PEPs, including obtaining senior management approval of such business relationships, taking measures to establish the sources of wealth and funds and conducting ongoing monitoring.
    - **Cross-border correspondent banking:** Appropriate steps must be taken to understand the respondent institution's business, reputation, supervision and AML controls; obtain management approval of such relationships; document the responsibilities of each institution; mitigate risks associated with payable-through accounts and ensure accounts are not established for shell banks.

- **Money or value transfer services (MVTs):** Countries should ensure that MVTs are licensed or registered and subject to appropriate AML requirements.
- **New technologies:** Countries and financial institutions should assess the risks associated with the development of new products, business practices, delivery mechanisms and technology. Financial institutions should assess these risks prior to launching new products; they should also take appropriate measures to mitigate the risks identified.
- **Wire transfers:** Countries should require financial institutions to obtain and send required and accurate originator, intermediary and beneficiary information with wires. Financial institutions should monitor wires for incomplete information and take appropriate measures. They should also monitor wires for those involving parties designated by the United Nations Security Council and take freezing actions or otherwise prohibit the transactions from occurring.
- **Suspicious transaction and/or activity reporting:** Financial institutions must report to the appropriate financial intelligence unit when they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing. The financial institutions and the employees reporting such suspicions should be protected from liability for reporting and should be prohibited from disclosing that they have reported such activity.
- **Expanded coverage of industries:** The Recommendations expand the fight against money laundering by adding new nonfinancial businesses and professions to the roster of financial institutions that are the usual focus of AML efforts. Expanding the scope of AML scrutiny is a key area where many governments have been aiming their AML arsenal in response to an increased flow of illicit money. These designated nonfinancial businesses and professions (DNFBPs) include
  - casinos when customers engage in financial transactions equal to or above a designated threshold. At a minimum, casinos should be licensed; authorities should prevent criminals from participating in casino operations and should supervise casinos to ensure compliance with requirements to combat money laundering and terrorist financing;
  - real estate agents when they are involved in transactions for clients concerning buying and selling properties;
  - dealers in precious metals and stones when they engage in any cash transaction with a customer at or above a designated threshold;
  - lawyers, notaries and independent legal professionals and accountants when they prepare or carry out transactions for clients concerning buying and selling real estate; managing client money, securities or other assets; establishing or managing bank, savings or securities accounts; organizing contributions for the creation or management of companies; creating, operating or managing legal persons or arrangements and buying and selling businesses; and
  - trust and company service providers when they prepare or carry out transactions for a client concerning certain activities (e.g., when acting as a formation agent of legal persons, acting as a director or secretary of a company, acting as a trustee of an express trust or acting as a nominee shareholder for another person).

FATF also designated specific thresholds that trigger AML scrutiny. For example, the threshold that financial institutions should monitor for occasional customers is \$15,000; for casinos, including internet casinos, it is \$3,000; and for dealers in precious metals, when engaged in any cash transaction, it is \$15,000.

- **Transparency and beneficial ownership of legal persons and arrangements:** Countries should take appropriate measures to prevent the misuse of legal persons for money laundering or terrorist financing, including ensuring information about the beneficial ownership and control of such legal persons is available to competent authorities, particularly with regard to legal persons who can issue bearer shares or have nominee shareholders or directors.
- **Powers and responsibilities of competent authorities:** Countries should oversee financial institutions to ensure they are implementing the FATF Recommendations and are not owned by or controlled by criminals. The supervisors should be given sufficient resources and powers to effectively oversee financial institutions within their jurisdictions. Designated nonfinancial businesses and people should be subject to oversight as well when they engage in certain financial activities. Countries should establish financial intelligence units and provide law enforcement and investigative authorities with sufficient resources and powers to investigate money laundering and terrorist financing and to seize or freeze criminal proceeds where found. Countries should implement measures to detect the physical cross-border movement of currency and bearer-negotiable instruments. The authorities should provide meaningful statistics, guidance and feedback on AML/CFT systems.
- **International cooperation:** Several Recommendations deal with strengthening international cooperation. Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in money laundering and terrorist financing investigations, freezing and confiscation of criminal proceeds, extradition and in other matters. Countries should ratify United Nations conventions against significant crimes and terrorism.

## FATF Members and Observers

---

FATF originally comprised 16 member jurisdictions. It has rapidly increased in membership and influence, now representing most major financial centers in all parts of the globe. Refer to the FATF-GAFI website for a current list of Members and Observers.



## FATF Membership Criteria

The following criteria are applied before considering a country as a potential candidate for FATF membership.

- a) The jurisdiction should be strategically important based on quantitative and qualitative indicators and additional considerations.

— *Quantitative Indicators*

- > Size of gross domestic product (GDP)
- > Size of the banking, insurance and securities sectors
- > Population

— *Qualitative Indicators*

- > Impact on the global financial system, including the degree of openness of the financial sector and its interaction with international markets
- > Active participation in a FATF-style regional body (FSRB) and regional prominence in AML/CFT efforts
- > Level of AML/CFT risks faced and efforts to combat those risks

— *Additional considerations*

- > Level of adherence to financial sector standards
- > Participation in other relevant international organizations

b) FATF's geographic balance should be enhanced by the jurisdiction becoming a member.

**Process for FATF Membership**

***Step 1—Engaging with the country and granting observership***

- a) The country should provide a written commitment at the political/ministerial level.
  - i. Endorsing and supporting the 2012 FATF Recommendations and the FATF AML/CFT Methodology 2013 (as amended from time to time)
  - ii. Agreeing to undergo a mutual evaluation during the membership process for the purposes of assessing compliance with FATF membership criteria, using the AML/CFT Methodology applicable at the time of the evaluation, as well as agreeing to submit subsequent follow-up reports
  - iii. Agreeing to participate actively in the FATF and to meet all the other commitments of FATF membership, including supporting the role and work of the FATF in all relevant fora
- b) The Plenary decides that a high-level visit to the country should be arranged in order to verify with the relevant ministers, representatives of the Parliament and competent authorities the written commitment, as well as to determine whether the country will be in a position to undergo a successful mutual evaluation and achieve a satisfactory level of technical compliance, including with the Recommendations essential for the establishment of a robust AML/CFT regime, such as Recommendations 3, 5, 10, 11 and 20 within 3 years. Consideration should also be given to the country's level of implementation of the essential Recommendations and its progress toward assessing and addressing its ML/TF risks, as called for in Recommendation 1. The high-level visit should include the president of the FATF, selected members of the Steering Group and heads of delegations. It is accompanied by the FATF Secretariat. The report of the high-level visit is presented at the following Plenary meeting.
- c) Based on the outcomes of the report of the high-level visit, the Plenary may decide to invite the country to participate in the FATF as an observer starting from the next Plenary meeting. If the Plenary decides not to invite the country to attend FATF meetings as an observer, it may decide to appoint a contact group to advise as to the appropriate time to extend such an invitation to the country. Then the contact group should engage with the competent authorities of the country to determine when the country will be in a position to undergo a successful mutual evaluation as mentioned in Step 2. The contact group is open to all FATF members and associate members and should include at least one member of the Steering Group. It is assisted by the FATF Secretariat. It will meet regularly and reports on the progress made by the country at each Plenary meeting.

***Step 2—Carrying out a mutual evaluation, agreeing on an action plan and granting membership***

Within a maximum of 3 years after being invited to participate in the FATF as an observer, the mutual evaluation process for the country should be launched. During this period, a new contact group may assist the country to ensure that it is ready for its mutual evaluation.

Membership is granted if the mutual evaluation is satisfactory. A mutual evaluation is not satisfactory if the country

- has eight or more NC/PC ratings for technical compliance;
- is rated NC/PC on any one or more of Recommendations 3, 5, 10, 11 and 20;
- has a low or moderate level of effectiveness for seven or more of the 11 effectiveness outcomes; or
- has a low level of effectiveness for four or more of the 11 effectiveness outcomes.

If the mutual evaluation is not satisfactory but is close to being satisfactory, then the country should provide a clear commitment at the political/ministerial level to reach the expected results within a reasonable timeframe (i.e., a maximum of 4 years). A detailed action plan setting out the steps to be taken and the timeframe for taking them is prepared by the country and reviewed by the second contact group before its adoption by the FATF Plenary.

At each FATF meeting, the Plenary closely monitors the implementation of the country's action plan.

- If it is not satisfied with the pace and/or extent of progress made, the Plenary can decide to apply to the country the enhanced measures listed under paragraph 77 of the procedures for the FATF fourth round of AML/CFT mutual evaluations.
- A country will not be granted full membership as long as it is rated NC/PC on any one or more of Recommendations 3, 5, 10, 11 or 20.
- Other than that, the Plenary may decide, at any time during the course of the completion of the action plan and in light of the progress made by the country to grant full membership before the action plan is completed.

**Noncooperative Countries**

Since its inception, FATF has had a practice of “naming and shaming” countries that it determines maintain inadequate anti-money laundering controls or are not cooperating in the global AML/CFT efforts. For years, FATF was engaged in an initiative to identify noncooperative countries and territories (NCCTs) in the global fight against money laundering. It developed a process to seek out critical weaknesses in specific jurisdictions’ anti-money laundering systems that obstruct international cooperation in this area.

On February 14, 2000, FATF published an initial report on noncooperative countries and territories that set out the 25 criteria that help identify relevant detrimental rules and practices and that are consistent with the 40 Recommendations. It described a process whereby jurisdictions having such rules and practices can be identified and encouraged to implement international standards in this area.

The 25 distinct criteria covered the following four broad areas.

1. Loopholes in financial regulations
  - No or inadequate regulations or supervision of financial institutions
  - Inadequate rules for the licensing or creation of financial institutions, including assessing the backgrounds of managers and beneficial owners
  - Inadequate customer identification requirements for financial institutions
  - Excessive secrecy provisions regarding financial institutions
  - Lack of efficient suspicious transactions reporting
2. Obstacles raised by other regulatory requirements
  - Inadequate commercial law requirements for registration of business and legal entities
  - Lack of identification of the beneficial owner(s) of legal and business entities
3. Obstacles to international cooperation
  - Obstacles to cooperation from administrative authorities
  - Obstacles to cooperation from judicial authorities
4. Inadequate resources for preventing and detecting money laundering activities
  - Lack of resources in public and private sectors
  - Absence of a financial intelligence unit or equivalent mechanism

The goal of the NCCT process was to reduce the vulnerability of the financial system to money laundering by ensuring that all financial centers adopt and implement measures for the prevention, detection and punishment of money laundering according to internationally recognized standards. The next step in the NCCT initiative was the publication in June 2000 of the first review identifying 15 NCCTs. The NCCT process ultimately involved 24 jurisdictions, including up to 19 jurisdictions at one time, until the jurisdictions eventually took the necessary steps to get off the list. At that point, FATF ceased the process.

The NCCT list was replaced by a new process when FATF started identifying jurisdictions with deficiencies in their AML/CFT regimes. This new FATF process was in response to the G-20 countries' efforts to publicly identify high-risk jurisdictions and to issue regular updates on jurisdictions with strategic deficiencies. Today, FATF identifies these jurisdictions in two public documents issued three times a year.

1. FATF's *Public Statement* identifies

- countries or jurisdictions with strategic deficiencies that are so serious that FATF calls on its members and non-members to apply counter-measures; and
- countries or jurisdictions for which the FATF calls on its members to apply enhanced due diligence measures proportionate to the risks arising from the deficiencies associated with the country.

2. *Improving Global AML/CFT Compliance: Ongoing Process* identifies countries or jurisdictions with strategic weaknesses in AML/CFT measures but that have provided a high-level commitment to an action plan developed with the FATF.

- FATF encourages its members to consider the strategic deficiencies identified within these jurisdictions.
- If a country fails to make sufficient or timely progress, FATF can increase its pressure on the country to make meaningful progress by moving it to the *Public Statement*.
- The document also provides information on jurisdictions no longer subject to FATF's ongoing global AML/CFT compliance process. Typically, a country is identified to have made significant progress in improving its AML/CFT regime when it establishes a legal and regulatory framework to meet its commitments in its action plan regarding the previously identified strategic deficiencies. However, the country must continue to work with the appropriate FATF-style regional body on addressing the items noted in its mutual evaluation report.

## The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision, established in 1974 by the central bank governors of the G-10 countries, promotes sound supervisory standards worldwide. The Committee is the primary global standard-setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability. The Committee's Secretariat is located at the Bank for International Settlements in Basel, Switzerland, and is staffed mainly by professional supervisors on temporary assignment from member institutions.

MEMBERS OF THE BASEL COMMITTEE ON BANK SUPERVISION	
COUNTRY	INSTITUTION
Argentina	Central Bank of Argentina
Australia	Reserve Bank of Australia Australian Prudential Regulation Authority
Belgium	National Bank of Belgium
Brazil	Central Bank of Brazil
Canada	Bank of Canada Office of the Superintendent of Financial Institutions

<b>MEMBERS OF THE BASEL COMMITTEE ON BANK SUPERVISION</b>	
<b>COUNTRY</b>	<b>INSTITUTION</b>
China	People's Bank of China China Banking Regulatory Commission
European Union	European Central Bank European Central Bank Single Supervisory Mechanism
France	Bank of France Prudential Supervision and Resolution Authority
Germany	Deutsche Bundesbank Federal Financial Supervisory Authority (BaFin)
Hong Kong SAR	Hong Kong Monetary Authority
India	Reserve Bank of India
Indonesia	Bank Indonesia Indonesia Financial Services Authority
Italy	Bank of Italy
Japan	Bank of Japan Financial Services Agency
Republic of Korea	Bank of Korea Financial Supervisory Service
Luxembourg	Surveillance Commission for the Financial Sector
Mexico	Bank of Mexico Comisión Nacional Bancaria y de Valores
Netherlands	Netherlands Bank
Russia	Central Bank of the Russian Federation
Saudi Arabia	Saudi Arabian Monetary Agency
Singapore	Monetary Authority of Singapore
South Africa	South African Reserve Bank
Spain	Bank of Spain
Sweden	Sveriges Riksbank Finansinspektionen
Switzerland	Swiss National Bank Swiss Financial Market Supervisory Authority FINMA
Turkey	Central Bank of the Republic of Turkey Banking Regulation and Supervision Agency
United Kingdom	Bank of England Prudential Regulation Authority
United States	Board of Governors of the Federal Reserve System Federal Reserve Bank of New York Office of the Comptroller of the Currency

OBSERVERS OF THE BASEL COMMITTEE ON BANK SUPERVISION	
COUNTRY	INSTITUTION
Chile	Central Bank of Chile Banking Financial Institutions Supervisory Agency
Malaysia	Central Bank of Malaysia
United Arab Emirates	Central Bank of the United Arab Emirates

## History of the Basel Committee

Banking supervisors are generally not responsible for the criminal prosecution of money laundering in their countries. However, they have an important role in ensuring that banks have procedures in place, including strict AML policies, to avoid involvement with drug traders and other criminals, as well as in the general promotion of high ethical and professional standards in the financial sector. The Bank of Credit and Commerce International (BCCI) scandal in the early 1990s, the indictments and guilty pleas of former officials of the Atlanta branch of the Italian Banca Nazionale del Lavoro in 1992 and other international banking scandals prompted banking regulators in the richest nations to agree on basic rules for the supervision and operation of multinational banks.

In 1988, the Basel Committee issued a Statement of Principles called *Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering* in recognition of the vulnerability of the financial sector to misuse by criminals. This was a step toward preventing the use of the banking sector for money laundering. The statement set out principles with respect to

- customer identification;
- compliance with laws;
- conformity with high ethical standards and local laws and regulations;
- full cooperation with national law enforcement to the extent permitted without breaching customer confidentiality;
- staff training; and
- record-keeping and audits.

These principles preceded AML legislation regarding the disclosure of client information to enforcement agencies and protection from civil suits brought by clients for breach of client confidentiality. Therefore, these principles stressed cooperation within the confines of confidentiality.

In 1997, the Basel Committee issued its *Core Principles for Effective Banking Supervision*, a basic reference for authorities worldwide. It stated that, “Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict ‘know-your-customer’ rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements.” It also urged nations to adopt FATF’s 40 Recommendations. The Core Principles were prepared with the assistance of 15 non-G-10 nations, including Brazil, Chile, Hong Kong, Mexico, Russia, Singapore and Thailand.

To facilitate implementation and assessment, the committee developed and published the *Core Principles Methodology* in October 1999. Since 1997, however, significant changes have occurred in banking regulation, much experience has been gained with implementing the Core Principles in individual countries, and new regulatory insights in regulation have become apparent. These developments made it necessary to update the Core Principles and the associated assessment methodology.

Based on the findings of an internal survey of cross-border banking conducted in 1999, the committee identified deficiencies in a large number of countries' know-your-customer (KYC) policies. "KYC policies in some countries have significant gaps and in others they are nonexistent. Even among countries with well-developed financial markets, the extent of KYC robustness varies," observed the committee in an October 2001 paper called *Customer Due Diligence for Banks*. The paper followed a consultation document issued in January 2001.

The committee's interest in KYC centers on the use of due diligence requirements to mitigate the dangers of bad customers. Without due diligence, banks can be subject to reputational, operational, legal and concentration risks, which can result in significant financial cost. Sound KYC policies and procedures are critical to protecting the safety and soundness of banks, as well as the integrity of banking systems. An example is the BCCI scandal that began in 1988 when nine BCCI officials were arrested in Florida for allegedly laundering drug money. It escalated and in 1991, BCCI was shut down by regulators, resulting in more than 70,000 creditors with admitted or in-progress claims that were valued at \$9 billion.

The committee's 2001 paper reinforced the principles established in earlier committee papers by providing more precise guidance on KYC standards and their implementation. In developing the guidance, the working group that wrote the paper drew on practices in member countries and took into account evolving supervisory developments. The essential elements presented in this paper are guidance as to minimum standards for worldwide implementation for all banks. However, these standards may need to be supplemented or strengthened with further measures tailored to the risks in particular institutions and in the banking system of individual countries. For example, enhanced due diligence is required for higher risk accounts and for banks that seek high net-worth customers. A number of specific sections in the paper offer recommendations for tougher standards of due diligence for higher risk areas within a bank.

The paper addresses

1. importance of KYC standards for supervisors and banks;
2. essential elements of KYC standards;
3. the role of supervisors; and
4. implementation of KYC standards in a cross-border context.

Specific issues emphasized in the paper include the following.

- The four key elements of a KYC program are
  1. customer identification;
  2. risk management;
  3. customer acceptance; and
  4. monitoring.

- Banks should not only establish the identity of their customers but should also monitor account activity to identify transactions that do not conform to the normal or expected transactions for that customer or type of account. “To ensure that records remain relevant, there is a need for banks to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated.”
- Numbered accounts should not be prohibited but be subjected to exactly the same KYC procedures as other customer accounts. KYC tests may be carried out by select staff, but the identity of customers must be known to an adequate number of staff if the bank is to be sufficiently diligent. “Such accounts should in no circumstances be used to hide the customer identity from a bank’s compliance function or from the supervisors.”
- Specific customer identification issues related to higher risk customers include
  - trust, nominee and fiduciary accounts;
  - corporate vehicles, particularly companies with nominee shareholders or entities with shares in bearer form;
  - introduced businesses;
  - client accounts opened by professional intermediaries, such as pooled accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds;
  - politically exposed persons;
  - non-face-to-face customers (i.e., customers who do not present themselves for a personal interview); and
  - correspondent banking.
- Banks should develop customer acceptance policies and procedures describing the customer’s background, country of origin, business activities and other risk indicators and should develop clear and concise descriptions of who is an acceptable customer.
- Private banking accounts should under no circumstances be allowed to escape KYC policies.
- Banks should make every effort to know the identity of corporations that operate accounts and, when professional intermediaries are involved, should verify the exact relationship between the owners and intermediary.
- Banks should use standard identification procedures when dealing with non-face-to-face customers and should never agree to open an account for persons who are adamant about anonymity.
- Periodic bank-wide employee training should be provided that explains the importance of the KYC policies and AML requirements.
- Internal auditors and compliance officials should regularly monitor staff performance and adherence to KYC procedures.

- Continued monitoring of high-risk accounts by compliance personnel should be conducted to obtain a greater understanding of the customers' normal activities and to enable the updating of identification papers and the detection of suspicious transaction patterns.
- Bank regulators should ensure that bank staff follow KYC procedures, review customer files and a sampling of accounts and emphasize that they will take appropriate action against officers who fail to follow KYC procedures.

Customer identification is an essential element of an effective customer due diligence program, which banks need in order to guard against reputational, operational, legal and concentration risks. It is also necessary in order to comply with AML legal requirements and to be able to identify bank accounts related to terrorism. In February 2003, the committee issued account opening and customer identification guidelines and a general guide to good practices based on the principles of the committee's paper, *Customer Due Diligence for Banks*. This document, which was developed by the working group on cross-border banking, does not cover every eventuality but instead focuses on some of the mechanisms that banks can use in developing an effective customer identification program.

The need for rigorous customer due diligence standards is not restricted to banks. The Basel Committee believes similar guidance needs to be developed for all nonbank financial institutions and professional intermediaries of financial services, such as lawyers and accountants.

In October 2004, the committee released another important publication on KYC, *Consolidated KYC Risk Management*, as a complement to its *Customer Due Diligence for Banks* issued in October 2001. The 2004 paper examines the critical elements for effective management of KYC risk throughout a banking group and addresses the need for banks to adopt a global approach and to apply the elements necessary for a sound KYC program to both the parent bank or head office and all of its branches and subsidiaries. These elements consist of risk management, customer acceptance and identification policies and ongoing monitoring of higher risk accounts.

In February 2016, the Basel Committee issued *Sound Management Of Risks Related To Money Laundering And Financing Of Terrorism* and its revised *General Guide to Account Opening*.

The guidelines on management of risks related to money laundering and the financing of terrorism describe how banks should include these risks within their overall risk management framework. The guidelines state that prudent management of these risks, together with effective supervisory oversight, is critical in protecting the safety and soundness of banks as well as the integrity of the financial system. Failure to manage these risks can expose banks to serious reputational, operational and compliance risks among others. The guidelines discuss the following issues.

- **Risk analysis and governance:** The first step in managing ML risks is to identify and analyze the risks, which will lead to the design and effective implementation of appropriate controls. The analysis should include appropriate inherent and residual risks at the country, sector, bank and business relationship level, among others. The assessment of risk should be documented and made available to authorities, such as supervisors. This assessment is also useful in scheduling discussions with other parties in the bank to help them see the risks and design the appropriate controls to mitigate them.

Another key aspect is proper governance arrangements, which create a culture of compliance with a strong tone from the top. The board of directors has a critical oversight role; as the senior-most management of the bank, they should approve and oversee policies for risk, risk management and compliance. The board also should have a clear understanding of the ML risks, including timely, complete and accurate information related to the risk assessment to make informed decisions. Along with senior management, the board should appoint a qualified chief AML officer with overall responsibility for the AML function and provide this senior-level officer with sufficient authority that when issues are raised they get the appropriate attention from the board, senior management and the business lines. This AML officer becomes the board's proxy for driving the day-to-day success of the bank's AML efforts, and as such, the board should provide the AML officer with sufficient resources to execute his or her responsibilities to oversee compliance with the bank's AML program.

- **Three lines of defense:** The committee describes three lines of defense in the bank's AML efforts: first, the line of business; second, compliance and internal control functions and third, internal audit.
  1. **The line of business** is responsible for creating, implementing and maintaining policies and procedures, as well as communicating these to all personnel. It must also establish processes for screening employees to ensure high ethical and professional standards and deliver appropriate training on AML policies and procedures based on roles and functions performed so employees are aware of their responsibilities. To facilitate this, employees should be trained as soon as possible after being hired, with refresher training as appropriate.
  2. **The AML compliance function**, as well as the larger compliance function, human resources and technology departments, are the second line of defence. In all cases, the AML officer is responsible for ongoing monitoring for AML compliance, including sample testing and a review of exception reports, to enable the escalation of identified noncompliance or other issues to senior management and, where appropriate, the board. The AML officer should be the contact point for all AML issues for internal and external authorities and should have the responsibility for reporting suspicious transactions. To enable the successful oversight of the AML program, the AML officer must have sufficient independence from the business lines to prevent conflicts of interest and unbiased advice and counsel. The officer should not be entrusted with the responsibilities of data protection or internal audit.
  3. **The audit function** should report to the audit committee of the board of directors (or similar oversight body) and independently evaluate the risk management and controls of the bank through periodic assessments, including the adequacy of the bank's controls to mitigate the identified risks, the effectiveness of the bank's staff's execution of the controls, the effectiveness of the compliance oversight and quality controls and the effectiveness of the training. The audit function must have knowledgeable employees with sufficient audit expertise. Audits should be conducted on a risk-based frequency; periodically, a bank-wide audit should be conducted. Audits should be properly scoped to evaluate the effectiveness of the program, including where external auditors are used. Auditors should proactively follow up on their findings and recommendations.

- **Customer due diligence and acceptance:** Banks should develop a customer acceptance policy to identify the customers that are likely to pose a higher ML risk (e.g., PEPs) as well as relationships that the bank will not accept (e.g., shell banks or those prohibited under economic sanctions, such as those imposed by the U.S. Office of Foreign Assets Control). Banks should apply basic due diligence to all customers and increase the due diligence as the risks increase. Some customers may be eligible for simplified due diligence where the ML risk is low, in accordance with applicable law.

Banks' CDD policies should address customer and beneficial owner identification, verification and risk profiling. As part of this, banks should identify customers and verify their identity, as well as that of beneficial owners. Banks should not establish a relationship or carry out transactions until the customer's identity has been verified, unless doing so would interrupt the normal conduct of business (in which case the bank should develop appropriate controls while verification and CDD is performed). Verification of identity should be through reliable means. For beneficial ownership, banks may use a written declaration from the customer but should not rely solely on such declarations.

Where CDD cannot be performed or customer identity verified, the bank should not open an account (or should close such opened accounts) and consider reporting such activity as suspicious to appropriate authorities. This applies to anonymous accounts as well; these should not be opened. If a bank allows for numbered accounts, these should not be allowed to serve as anonymous accounts; sufficient personnel should have full access to the information to ensure appropriate CDD on and oversight over these accounts.

- **Transaction monitoring systems and ongoing monitoring:** Because the transactional monitoring system is key to mitigating ML risk within the bank, the committee recognizes that AML risks require more than just appropriate policies and procedures; banks must have adequate and appropriate monitoring systems. For most banks, this will involve an IT monitoring system. If the bank does not believe it needs an IT monitoring system, it should document the rationale for why it does not need one. The monitoring system should cover all accounts and transactions of the bank's customers and enable a trend analysis of activity and identify unusual business relationships and transactions, particularly with regard to changes in the transactional profile of customers. The IT system should allow the bank to gain a centralized knowledge of information, for example organized by customer, by legal entity within a larger group and/or by business unit. Although the guidance indicates a bank must have a system, it should be understood that this does not mean that there can only be one IT tool that will do all of this; rather, the tools must be able to work together to enable the bank to gain an enterprise-level view of ML risk across the bank.

A critical way to mitigate ML risk is by using the transaction monitoring system to conduct ongoing monitoring of customer activity, building on the information from risk assessments and customer profiles. This enables banks to satisfy their obligation to identify and report suspicious activity. Monitoring systems should be adapted to the risks present in the bank, such as if the bank identifies a particular money laundering scheme occurring within its jurisdiction.

- **Management of information:** Because one of the primary purposes of AML rules is to create records that enable law enforcement to trace financial transactions back to the people who conduct them, banks should retain records. Banks should both record the documents they are provided when verifying customer/beneficial owner identity, whether a photocopy of the document or by recording information from the document or nondocumentary source, and enter all CDD information into their IT systems. The CDD information should be kept up to date and accurate, which will mean periodically assessing the information, generally on a risk-based frequency.

Banks should also document decisions related to investigations of unusual activity, whether a decision is made to file a report of suspicious activity or not. Banks should maintain all of these records as required by law, for at least 5 years after closure of the account. If an ongoing investigation is occurring, relevant CDD records should not be destroyed merely because the record retention period has expired.

- **Reporting of suspicious transactions and asset freezing:** Ongoing monitoring of accounts and transactions will enable banks to identify unusual activity, refer unusual activity to an internal review function, eliminate false positives and report suspicious activity in a timely and confidential manner. This process should be clearly spelled out in policies and procedures and communicated to appropriate staff.

Where suspicious activity has been reported, the bank should take appropriate action regarding the customer, including raising the risk rating of the customer and/or deciding whether to retain the relationship (either the account or the entire relationship). In some cases, it may make sense to close out one account but not the whole relationship, such as when a customer has both a checking account and an outstanding loan. Banks should screen new customers against applicable sanctions lists and the existing portfolio against changes to the sanctions list to identify relationships that may need to be frozen. Banks should have a means of properly freezing any assets identified as part of this process.

## European Union Directives on Money Laundering

---

### FIRST DIRECTIVE

The First European Union Directive, *Money Laundering: Preventing Use of the Financial System* (Directive 91/308/EEC), was adopted by the Council of the European Communities in June 1991.

Like all directives adopted by the Council, it required member states to achieve (by amending national law, if necessary) the specified results. This First Directive required the members to enact legislation to prevent their domestic financial systems from being used for money laundering.

The unique nature of the EU as a community of states makes it fundamentally different from other international organizations. The EU can adopt measures that have the force of law even without the approval of the national parliaments of the various member states. Plus, European law prevails over national law in the case of directives. In this respect, EU Directives have far more weight than the voluntary standards issued by groups such as the Basel Committee or FATF. Of course, the Directive applies only to EU member states and not to other countries.

The First Directive of 1991 confined predicate offenses of money laundering to drug trafficking as defined in the 1988 Vienna Convention. However, member states were encouraged to extend the predicate offenses to other crimes.

## SECOND DIRECTIVE

In December 2001, the EU agreed on a Second Directive (Directive 2001/97/EEC) that amended the first one to require stricter money laundering controls across the continent.

Member states agreed to implement it as national law by June 15, 2003; however, only Denmark, Germany, the Netherlands and Finland met the deadline, with Ireland and Spain complying shortly afterwards. Other member states eventually followed.

The following were the key features of the Second Directive.

- It extended the scope of the First Directive beyond drug-related crimes. The definition of criminal activity was expanded to cover not just drug trafficking, but all serious crimes, including corruption and fraud against the financial interests of the European community.
- It explicitly brought bureaux de change and money remittance offices under AML coverage.
- It clarified that knowledge of criminal conduct can be inferred from objective factual circumstances.
- It provided a more precise definition of money laundering to include
  - the conversion or transfer of property with knowledge that it is derived from criminal activity or from participation in that activity, for the purpose of concealing or disguising the illicit origin of the property, or assisting anyone who is involved in the commission of the activity to evade the legal consequences of his action;
  - concealing or disguising the nature, source, location, disposition, movement, rights with respect to or ownership of property, knowing that the property is derived from criminal activity or from an act of participation in that activity;
  - the acquisition, possession, or use of property knowing, when it is received, that it was derived from criminal activity or from an act of participation in the activity; and
  - participation in, association to commit, the attempt to commit and the aiding, abetting, facilitating or counseling the commission of any of the mentioned actions.
- It widened the businesses and professions that are subject to the obligations of the Directive. Certain persons, including lawyers when they participate in the movement of money for clients, were required to report to authorities any fact that might indicate money laundering. Covered groups included auditors, external accountants, tax advisers, real estate agents, notaries and legal professionals.

The Second Directive was a tremendous step forward because its applicability included many of the important financial centers of the world. It went well beyond similar standards issued by other organizations, such as the U.N. and even FATF.

## THIRD DIRECTIVE

A Third EU Directive, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Directive 2005/60/EC), based on elements of FATF's revised 40 Recommendations, was adopted in 2005.

The Third Directive was to be implemented by member states by December 15, 2007. Although several countries did not meet this original deadline, the Directive was eventually implemented by all members.

In line with FATF's anti-money laundering recommendations, the Third EU Directive extended the scope of the First and Second Directives by

- defining money laundering and terrorist financing as separate crimes. The directive's measures were expanded to cover not only the manipulation of money derived from crime but also the collection of money or property for terrorist purposes;
- extending customer identification and suspicious activity reporting obligations to trusts and company service providers, life insurance intermediaries, and dealers selling goods for cash payments of more than 15,000 euros;
- detailing a risk-based approach to customer due diligence. The extent of due diligence that is performed on customers, whether simplified or enhanced, should be dependent on the risk of money laundering or terrorist financing they pose;
- protecting employees who report suspicions of money laundering or terrorist financing. This provision instructs member states to "do whatever is in their power to prevent employees from being threatened";
- obligating member states to keep comprehensive statistics regarding the use of and results obtained from suspicious transaction reports, such as the number of suspicious transaction reports filed; the follow-up given to those reports; and the annual number of cases investigated, persons prosecuted and persons convicted; and
- requiring all financial institutions to identify and verify the beneficial owner of all accounts held by legal entities or persons. "Beneficial owner" refers to the natural person who directly or indirectly controls more than 25 percent of a legal entity or person.

The Third Money Laundering Directive applies to

- credit institutions;
- financial institutions;
- auditors, external accountants and tax advisors;
- legal professionals;
- trust and company service providers;
- estate agents;
- high-value goods dealers who trade in cash over 15,000 euros; and
- casinos.

The scope of the Third Directive differs from the Second Directive in that

- it specifically includes the category of trust and company service providers;
- it covers all dealers trading in goods who trade in cash over 15,000 euros; and
- the definition of financial institution includes certain insurance intermediaries.

There were three main points of contention with regard to the Third Directive.

1. The definition of politically exposed persons (PEPs). The Third Directive defined PEPs as “natural persons who are or have been entrusted with prominent public functions and the immediate family members, or individuals known to be close associates, of such persons.” Close associates must be identified only when their relationship with a PEP is publicly known or when the institution suspects there is a relationship. Finally, the commission said persons should not be considered PEPs after 1 year of not being in a prominent position.
2. The inclusion of lawyers among those who are required to report suspicious activity.
3. The precise role of a comitology committee. The European Commission coined the term “comitology,” which means the EU system that oversees the implementation of acts proposed by the European Commission.

## FOURTH DIRECTIVE

Directive (EU) 2015/849 of the European Parliament and of the Council of 20, May 2015, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, entered into effect on June 26, 2015. Member states had 2 years from that date to adapt their national legislations accordingly. This directive repealed the Third Directive and its predecessors.

Changes in the Fourth Money Laundering Directive include the following.

- Natural or legal persons trading in goods will be covered to the extent that they make or receive cash payments of EUR 10,000 or more (decreased from EUR 15,000)
- The scope of obliged entities was enlarged from just casinos to all “providers of gambling services.”
- Customer due diligence is to be applied for transfers of funds exceeding 1,000 euros.
- New definitions for
  - correspondent relationship;
  - PEPs’ family members and persons known to be close associates; and
  - senior management and others.
- Tax crimes relating to direct and indirect taxes are included in the broad definition of criminal activity, in line with the revised FATF Recommendations.
- An explanation of “financial activity on an occasional or very limited basis” was included.
- The European Commission must submit a report every 2 years on the findings of the risk assessment of ML and TF affecting the internal market.

- The EU executive is also in charge of identifying third-country jurisdictions having strategic deficiencies with regard to AML and CFT (i.e., high-risk third countries).
- Special attention is given to PEPs. In this regard, enhanced due diligence (EDD) should be applied to every PEP, whether the individual is a domestic or third-country citizen. The risk these people pose is for at least 12 months and measures they are subject to must also be applied to their family members and their known close associates.
- For groups (and their branches and subsidiaries), this directive sets the criteria for adequate compliance related to third parties for customer due diligence.
- New requirements regarding beneficial ownership information have been introduced, particularly for trusts and similar legal arrangements. Subject to data protection rules, this information must be held in central registers in each member state and must be made available to competent authorities, financial intelligence units (FIUs), obliged entities and any person with legitimate interest.
- Data in the statistics relevant to the effectiveness of systems to combat ML and TF were enlarged to include, for instance, size and importance of sectors or the number of cross-border requests for information dealt with by FIUs.
- Obligated entities that are part of a group are required to implement group-wide policies and procedures as well as to take measures proportionate to their risks. Criminals or their associates, convicted in relevant areas, are prevented from holding management functions or indirectly controlling certain obliged entities.
- With regard to penalties for breach of the provisions, the set of administrative sanctions and measures now range from “name and shame” to withdrawal of authorization. Pecuniary sanctions for natural persons are set to at least 5 million euros or 10 percent of the total annual turnover for entities.
- An entire section of the directive is dedicated to the rules for cooperation between member state FIUs, the European Supervisory Authorities (ESAs) and the EU Commission.
- Because it is a directive and not a regulation, this legislative act gives some discretion to member states on the application of the provisions.
- At the national level, the Directive requests that member states conduct an ML/TF risk assessment as well as designate a responsible authority. Moreover, they must ensure that obliged entities take appropriate steps to identify and assess their own risks. Nonexhaustive lists of potentially lower and higher risks are provided for guidance in these risk assessments and are based on
  - customer risk factors, such as public administrations versus cash-intensive businesses;
  - product/service, transaction or delivery channel risk factors, such as low premium insurance policies versus private banking; and
  - geographical risk factors, such as member states versus countries subject to sanctions.

## OTHER RELEVANT LEGAL DOCUMENTS

In addition to the above-mentioned laws, the EU legislation on AML and CFT includes the following.

- Joint Action (1998) on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime and its subsequent amendment
- Framework Decision (2001)
- Framework Decision (2000) on European FIUs', cooperation
- Regulation (2001) on restrictive measures for combating terrorism and its amending Regulation (2003)
- Cash Control Regulation (2005)
- Wire Transfer Regulation (2015)

## FATF-Style Regional Bodies

---

### FATF-STYLE REGIONAL BODIES AND FATF ASSOCIATE MEMBERS

There are nine FATF-style regional bodies (FSRBs) that have similar form and functions to those of FATF. They are also considered FATF associate members. In setting standards, FATF depends on input from the FSRBs as much as from its own members; however, FATF remains the only standard-setting body.

The following high-level principles apply for both FATF and FSRBs.

- **Role:** FSRBs play an essential role in identifying and addressing AML/CFT technical assistance needs for their individual members. In those FSRBs that carry out this coordination work, technical assistance necessarily complements mutual evaluation and follow-up processes by helping jurisdictions to implement FATF standards.
- **Autonomy:** FATF and FSRBs are free-standing organizations that share the common goals of combating money laundering and the financing of terrorism and proliferation and of fostering effective AML/CFT systems.
- **Reciprocity:** FATF and FSRBs operate on the basis of (mutual or joint or common) recognition of their work, which implies that FSRBs and FATF put in place similar mechanisms for effective participation and involvement in each other's activities.
- Because FATF and FSRBs are part of a larger whole and the success or failure of one organization can have an effect on all organizations, protection of the FATF brand is in the common interest of both FATF and FSRBs.

Many FATF member countries are also members of the nine FSRBs.

- Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)

- Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL, formerly PC-R-EV)
- Eurasian Group (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Financial Action Task Force of Latin America (GAFILAT) (formerly known as Financial Action Task Force on Money Laundering in South America (GAFISUD))
- Intergovernmental Action Group against Money Laundering in West Africa (GIABA)
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- Task Force on Money Laundering in Central Africa (GABAC)

## ASIA/PACIFIC GROUP ON MONEY LAUNDERING (APG)

The APG, an autonomous regional anti-money laundering body, was established in February 1997 at the Fourth Asia/Pacific Money Laundering Symposium in Bangkok, where it adopted its *Terms of Reference*.

The *Terms of Reference* were substantially revised in July 2012 to recognize that the FATF's revised 40 Recommendations constituted the new international standards on combating money laundering and the financing of terrorism and proliferation. The Terms included a commitment that APG members would implement these recommendations according to their particular cultural values and constitutional frameworks. It also said that to ensure a global approach members of the APG would work closely with FATF.

The APG

- provides a focus for cooperative AML/CFT efforts in the Asia/Pacific region;
- provides a forum in which
  - regional issues can be discussed and experiences shared, and
  - operational cooperation among member jurisdictions is encouraged;
- facilitates the adoption and implementation by member jurisdictions of internationally accepted AML/CFT measures;
- enables regional and jurisdictional factors to be taken into account in the implementation of international AML/CFT measures;
- encourages jurisdictions to implement AML/CFT initiatives, including more effective mutual legal assistance; and
- coordinates and provides practical support, where possible, to member and observer jurisdictions in the region, when requested.

The APG is voluntary and cooperative in nature. The work done by the APG and its procedures are decided by mutual agreement among its members. The group was established by agreement among its members and is autonomous. It is not derived from an international treaty and is not part of any international organization.

The APG also uses similar mechanisms to those used by FATF to monitor and facilitate progress. The APG and FATF have reciprocal rights of attendance at each other's meetings, as well as reciprocal sharing of documents. However, the APG, as with other autonomous AML bodies, determines its own policies and practices. It is not a precondition for participation in the APG that AML/CFT laws already be enacted.

The APG has seen its membership grow from its original 13 founding members in 1997 to 41 members as of July 2015. APG members include Afghanistan, Australia, Bangladesh, Bhutan, the Kingdom of Brunei Darussalam, Cambodia, Canada, China, the Cook Islands, Fiji, Hong Kong (China), India, Indonesia, the Republic of Korea (South Korea), Japan, Lao People's Democratic Republic, Macao (China), Malaysia, Maldives, The Marshall Islands, Mongolia, Myanmar, Nauru, Nepal, New Zealand, Niue, Pakistan, Palau, Papua New Guinea, The Philippines, Samoa, Singapore, Solomon Islands, Sri Lanka, Chinese Taipei, Thailand, Timor Leste, Tonga, the United States of America, Vanuatu and Vietnam.

The APG Secretariat is headquartered in Sydney, Australia. The APG can be located online at [www.apgml.org](http://www.apgml.org).

## **CARIBBEAN FINANCIAL ACTION TASK FORCE (CFATF)**

Given its proximity to the world's largest cocaine producers and exporters in South America's Andean region and one of the largest drug markets (the U.S.), the Caribbean basin has long been a convenient banking center for many international criminals, including drug dealers.

The group consists of 27 states in the Caribbean Basin and Central and South America that have agreed to implement common countermeasures to address the problems of money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. It was established as the result of meetings convened in Aruba in May 1990 and Jamaica in November 1992.

The main objective of the CFATF is to achieve effective implementation of and compliance with its recommendations to prevent and control money laundering and to combat the financing of terrorism. The Secretariat has been established as a mechanism to monitor and encourage progress to ensure full implementation of the Kingston Ministerial Declaration (*see below*).

In May 1990, representatives of Western Hemisphere countries, in particular from the Caribbean and from Central America, convened in Aruba to develop a common approach to the phenomenon of the laundering of the proceeds of crime. Nineteen recommendations constituting this common approach were formulated. These recommendations, which had specific relevance to the region, were seen as complementary to FATF's 40 Recommendations.

The Jamaica Ministerial Meeting was held in Kingston in November 1992. Ministers issued the Kingston Ministerial Declaration in which they endorsed and affirmed their governments' commitment to implement the FATF and Aruba Recommendations, the Organization of American States

(OAS) Model Regulations and the 1988 UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. They also mandated the establishment of the Secretariat to coordinate the implementation of these by CFATF member countries.

The Declaration recommended laws

- defining money laundering based on the model laws issued by the Organization of American States;
- concerning the seizure and forfeiture of drug proceeds and linked assets that enable the identification, tracing and evaluation of property subject to seizure and that permit freezing orders;
- allowing judicial challenges to seizure orders by an administrative body;
- permitting forfeiture in all cases following conviction; and
- permitting courts to decide that “all property obtained during a prescribed period of time by a person convicted of drug trafficking has been derived from such criminal activity.”

The Caribbean nations agreed to enter into mutual assistance agreements with each other to assist in money laundering investigations. They also agreed that money laundering should be an extraditable offense subject to simplified procedures and that forfeited assets should be shared among cooperating nations.

CFATF members include Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Curaçao, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Guyana, Haiti, Jamaica, Montserrat, St. Kitts and Nevis, St. Lucia, St. Maarten, St. Vincent and the Grenadines, Suriname, Trinidad and Tobago, Turks and Caicos Islands and Venezuela.

The CFATF monitors members’ implementation of the anti-money laundering recommendations. The CFATF Secretariat is hosted by the Government of Trinidad and Tobago. The CFATF can be located online at <https://www.cfatf-gafic.org/>.

## **COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES (MONEYVAL)**

In September 1997, MONEYVAL was established by the Committee of Ministers of the Council of Europe to conduct self- and mutual-assessment exercises of the AML measures in place in Council of Europe member states that were not members of FATF. MONEYVAL became an associate member of FATF in 2006.

On October 13, 2010, the Committee of Ministers adopted the Resolution CM/Res(2010)12 on the Statute of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). The statute elevated MONEYVAL to an independent monitoring mechanism within the Council of Europe, answerable directly to the Committee of Ministers on January 1, 2011. The MONEYVAL Statute was further amended in 2013 by the Resolution CM/Res(2013)13.

MONEYVAL members include: Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Gibraltar\*, Georgia, Guernsey\*, Hungary, Holy See (since April 2011)\*, Isle of Man\*, Israel (since January 2006)\*, Jersey\*, Latvia, Liechtenstein, Lithuania, Malta, Moldova, Monaco, Montenegro, Poland, Romania, Russian Federation (also a FATF member since 2003), San Marino, Serbia, Slovak Republic, Slovenia, the former Yugoslav Republic of Macedonia and Ukraine.

*\*Nonmembers of the Council of Europe.*

MONEYVAL is hosted by the Council of Europe in Strasbourg, France. MONEYVAL is located online at [www.coe.int/t/dghl/monitoring/moneyval/](http://www.coe.int/t/dghl/monitoring/moneyval/).

## **FINANCIAL ACTION TASK FORCE OF LATIN AMERICA (GAFILAT)**

The Financial Action Task Force of Latin America (GAFILAT), formerly known as Financial Action Task Force on Money Laundering in South America (GAFISUD), was created in December 2000 in Cartagena de Indias, Colombia, when a Memorandum of Understanding was signed by government representatives from nine countries: Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru and Uruguay. Mexico (2006), Costa Rica and Panama (2010), Cuba (2012), Guatemala, Honduras and Nicaragua (2013) have since joined as plenary members.

GAFILAT was created in the style of FATF and accepts its 40 Recommendations as the international standard against money laundering and terrorist financing. It also develops enhanced recommendations to improve national policies against those crimes.

GAFILAT supports its members in the implementation of the 40 Recommendations as national legislation and the creation of a regional prevention system against money laundering and terrorist financing. The two main tools are training measures and mutual evaluations.

GAFILAT members include: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru and Uruguay.

GAFILAT has legal capacity and diplomatic status in the Argentine Republic where its Secretariat is located. GAFILAT can be located online at <http://www.gafilat.org/index.php>.

## **INTERGOVERNMENTAL ACTION GROUP AGAINST MONEY LAUNDERING IN WEST AFRICA (GIABA)**

GIABA was established on December 10, 1999, by a decision of the Authority of Heads of State and government of the Economic Community Of West African States (ECOWAS). In January 2006, GIABA revised its mandate to fully incorporate and properly reflect its fight against the financing of terrorism.

The objectives of GIABA are to

- protect the national economies and the financial and banking systems of signatory states against the proceeds of crime and the financing of terrorism;
- improve measures and intensify efforts to combat the proceeds from crime; and
- strengthen cooperation amongst its members;

GIABA members include Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea Bissau, Guinea Conakry, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

GIABA's Secretariat is located in Senegal, West Africa and can be located online at [www.giaba.org](http://www.giaba.org).

## **MIDDLE EAST AND NORTH AFRICA FINANCIAL ACTION TASK FORCE (MENAFATF)**

At an inaugural Ministerial Meeting held in Manama, Bahrain, in November 2004, the governments of 14 countries decided to establish a FATF-style regional body for the Middle East and North Africa. The MENAFATF is voluntary in nature and was established by agreement between its members. It is not derived from an international treaty. It is independent of any other international organization and sets its own work, rules and procedures, which are determined by consensus of its members. It cooperates with other international bodies, notably FATF, to achieve its objectives.

Member countries of MENAFATF agreed on the following objectives and are working towards achieving them.

- To adopt and implement FATF's 40 Recommendations against money laundering and terrorist financing and proliferation, as well as the related U.N. Conventions and U.N. Security Council Resolutions as the accepted international standards in this regard, in addition to any other standards that are adopted by Arab states to enhance the fight against money laundering and the financing of terrorism and proliferation in the region
- To implement the relevant U.N. treaties and agreements and U.N. Security Council Resolutions dealing with fighting money laundering and terrorist financing
- To cooperate to raise compliance with these standards and measures within the MENA region and to work with other international organizations to raise compliance worldwide
- To work together to identify regional money laundering and terrorist financing issues, to share experiences with these problems and to develop regional solutions for dealing with them
- To build effective arrangements and systems throughout the region to effectively fight money laundering and terrorist financing that do not contradict with the cultural values, constitutional frameworks and legal systems of the member countries

MENAFATF members include Algeria, Bahrain, Egypt, Islamic Republic of Mauritania, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Palestinian Authority, Qatar, Republic of Iraq, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates and Yemen.

MENAFATF is headquartered in Bahrain and can be located online at [www.menafatf.org](http://www.menafatf.org).

## **EURASIAN GROUP ON COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM (EAG)**

The Eurasian Group (EAG) was formed in October 2004 in Moscow. The EAG was created for the countries of the Eurasian region not included in the existing FATF-style regional groups.

The primary goals of EAG are to ensure effective interaction and cooperation at the regional level and integration of EAG member states into the international AML/CFT system in accordance with FATF's 40 Recommendations as well as the standards of other international organizations to which EAG member states are party.

The main tasks of EAG are

- assisting member states in implementing the FATF Recommendations;
- developing and conducting joint activities aimed at combating money laundering and terrorist financing;
- implementing a program of mutual evaluations of member states based on the FATF Recommendations, including assessment of the effectiveness of legislative and other measures adopted in the sphere of AML/CFT efforts;
- coordinating international cooperation and technical assistance programs with specialized international organizations, bodies and interested states; and
- analyzing money laundering and terrorist financing trends (typologies) and exchanging best practices of combating such crimes taking into account regional specifics.

The EAG members include Belarus, China, India, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan and Uzbekistan.

The EAG is headquartered in Moscow, Russian Federation, and can be located online at <http://www.eurasiangroup.org/>.

## **EASTERN AND SOUTH AFRICAN ANTI-MONEY LAUNDERING GROUP (ESAAMLG)**

The Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) is an intergovernmental body whose mandate is to promote the effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other threats to the integrity of the international financial system.

Launched in Tanzania in 1999, current membership in the ESAAMLG comprises 18 countries: Angola, Botswana, Comoros, Ethiopia, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Rwanda, Seychelles, South Africa, Swaziland, Tanzania, Uganda, Zambia and Zimbabwe.

The main decision-making body of the ESAAMLG is the Council of Ministers, which comprises state member ministers dealing with matters relating to finance.

The group developed a Memorandum of Understanding among its member countries, in which they agreed to

- adopt and implement the 40 FATF Recommendations;
- apply AML measures to all serious crimes;
- implement measures to combat the financing of terrorism; and

- implement any other measures contained in multilateral agreements and initiatives to which they subscribe for the prevention and control of the laundering of the proceeds of all serious crimes and the financing of terrorist activities.

Region-specific projects and studies are undertaken by the ESAAMLG. For example, a project was initiated in 2014 aiming to obtain information, statistics and trends related to wildlife poaching, illegal trade in wildlife products and associated money laundering.

ESAAMLG is headquartered in Tanzania and can be located online at [www.esaamlg.org](http://www.esaamlg.org).

### **TASK FORCE ON MONEY LANDERING IN CENTRAL AFRICA (GABAC)**

The Task Force on Money Laundering in Central Africa known as *Groupe d'Action contre le blanchiment d'Argent en Afrique Centrale* (GABAC) is a body of the Economic and Monetary Community of Central Africa. Established in 2000, its mandate is to combat money laundering and terrorist financing, assess the compliance of its members against FATF standards, provide technical assistance to its member states and facilitate international cooperation. In February 2012, GABAC became an observer organization of FATF. In October 2015, FATF recognized GABAC as an FSRB and admitted it as an Associate Member.

GABAC members include Cameroon, Central African Republic, Chad, Republic of the Congo, Equatorial Guinea and Gabon.

GABAC is headquartered in Bangui, Central Africa and can be located online at [www.spgabac.org](http://www.spgabac.org).

### **Organization of American States: Inter-American Drug Abuse Control Commission (Comisión Interamericana Para El Control Del Abuso De Drogas)**

---

In May 1992, the Organization of American States (OAS) became the first permanent international body to reach an agreement on model legislation aimed specifically at dealing with money laundering. At its annual general assembly held in Nassau, the Bahamas, the OAS unanimously approved a set of 19 articles written in statutory language that it recommended its member nations enact.

The OAS action was not an overnight affair. The vote was the culmination of a 2-year effort by the Inter-American Drug Abuse Control Commission, an OAS entity that goes by the acronym CICAD (Comisión Interamericana para el Control del Abuso de Drogas). In 1990, CICAD gathered a group of experts from 14 nations to craft the articles.

#### **CICAD**

- serves as the Western Hemisphere's policy forum on all aspects of the drug problem;
- fosters multilateral cooperation on drug issues in the Americas;
- executes action programs to strengthen the capacity of member states to prevent and treat drug abuse, to combat production and trafficking of illicit drugs and to deny traffickers their ill-gotten gains;

- promotes drug-related research, information exchange, specialized training and technical assistance;
- develops and recommends minimum standards for drug-related legislation, treatment, measurement of both drug consumption and the cost of drugs to society and drug-control measures, among others; and
- carries out regular multilateral evaluations of progress by member states in all aspects of the drug problem.

CICAD's core mission is to strengthen the human and institutional capabilities and to harness the collective energy of member states to reduce the production, trafficking and use of illegal drugs in the Americas and to address the health, social and criminal repercussions of the drug trade.

Within CICAD is an Anti-Money Laundering Unit (CICAD-AMLU), established in 1999. The Unit focuses its efforts on providing technical assistance and training to all member states in judicial and financial measures and law enforcement. It also acts as Secretariat of CICAD's Group of Experts for the Control of Money Laundering.

Through the Group of Experts, Model Regulations are developed on money laundering offenses related to drug trafficking and other crimes including the financing of terrorism. These regulations serve as permanent legal documents providing a legal framework to member states. They were influenced by and are compatible with FATF's 40 Recommendations.

The entire set of Model Regulations is available at: <http://www.cicad.oas.org>.

In 1999, the Inter-American Development Bank (IADB) and CICAD started a program in eight South American countries to train employees from financial institutions and from the financial regulatory agencies responsible for enforcing anti-money laundering requirements. In 2001, another program was developed and conducted for judges and prosecutors within the eight countries, and in 2002, a long-term project was begun to establish financial intelligence units in Argentina, Chile, Ecuador, Brazil, Peru, Uruguay and Venezuela.

CICAD can be located online at <http://www.cicad.oas.org>.

## **Egmont Group of Financial Intelligence Units**

---

In 1995, a number of national financial intelligence units (FIUs) began working together in an informal organization known as the Egmont Group (named for the location of the first meeting, the Egmont-Arenberg Palace in Brussels). The goal of the group is to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field.

This support includes

- expanding and systematizing cooperation in the reciprocal exchange of information;
- increasing the effectiveness of FIUs by offering training and promoting personnel exchanges to improve the expertise and capabilities of personnel employed by FIUs;

- fostering better and secure communication among FIUs through the application of technology, such as the Egmont Secure Web (ESW);
- promoting the operational autonomy of FIUs; and
- promoting the establishment of FIUs in conjunction with jurisdictions with an AML/CFT program in place, or in areas with a program in the early stages of development.

The Egmont Group comprises several organizational groups: The Heads of FIUs (HoFIUs), the Egmont Committee, the Working Groups, the Regional Groups and the Egmont Group Secretariat. The five working groups that meet periodically and report to the Heads of FIUs include the IT Working Group (ITWG), Legal Working Group (LWG), Operational Working Group (OpWG), Outreach Working Group (OWG) and Training Working Group (TWG).

In 2013, the Egmont Group produced a revised set of governing documents to lay the foundation for the future work of the Egmont Group and contribute to greater international cooperation and information exchange between FIUs. These documents include The Egmont Charter, Egmont Principles for Information Exchange and Operational Guidance for FIUs.

Resources provided by the Egmont Group include case studies related to money laundering, terrorist financing, fraud and other forms of financial crimes. These case studies often consist of information compiled by reviewing cases submitted by FIUs from various jurisdictions and can be used to assist AML professionals in identifying suspicious activity and determining whether or not to report these activities.

In 1999, the TWG undertook an initiative that resulted in Egmont's publishing of *FIUs in Action: 100 Sanitised Cases*. According to the Egmont Group, the publication has provided invaluable assistance in identifying the components of money laundering cases. Beyond the analysis of the 100 cases, the report identified six of the most frequently observed indicators of money laundering.

1. Large-scale cash transactions.
2. Atypical or uneconomical fund transfers to or from a foreign jurisdiction.
3. Unusual business activity or transactions.
4. Large and/or rapid movements of funds.
5. Unrealistic wealth compared to client profile.
6. Defensive stance to questioning.

As of 2015, there were 151 Egmont member FIUs and 19 observer organizations. The group is expected to continue to grow because as per the 2012 FATF Recommendations, it is expected that FIUs apply for membership. The Egmont Group can be located online at <http://www.egmontgroup.org/>.

## The Wolfsberg Group

---

The Wolfsberg Group is an association of 13 global banks that aims to develop financial services industry standards and guidance related to know your customer anti-money laundering and counter-terrorist financing policies. The Wolfsberg Group, which has no enforcement powers, issued the guidelines to manage its members' own risks to help make sound decisions about clients and to protect their operations from criminal abuse.

The Group first came together in 2000 at the Wolfsberg castle in Switzerland, accompanied by representatives of Transparency International, to draft anti-money laundering guidelines for private banking that, when implemented, would mark an unprecedented private-sector assault on the laundering of corruption proceeds.

The Wolfsberg *Anti-Money Laundering Principles for Private Banking* was published in October 2000 and was revised in May 2002 and again in June 2012. These principles recommend controls for private banking that range from the basic, such as customer identification, to enhanced due diligence, such as heightened scrutiny of individuals who “have or have had positions of public trust.” The banks that released the principles with Transparency International said that the principles would “make it harder for corrupt people to deposit their ill-gotten gains in the world’s banking system.”

The principles state that banks must “endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate.” They highlight the need to identify the beneficial owner of funds “for all accounts” when that person is someone other than the client and urge private bankers to perform due diligence on “money managers and similar intermediaries” to determine that the middlemen have a satisfactory due diligence process for their clients or a regulatory obligation to conduct such due diligence. The principles recommend that “at least one person other than the private banker” should approve all new clients and accounts.

The Principles list several situations that require enhanced due diligence, including activities that involve

- politically exposed persons, such as public officials, holding or having held “senior, prominent or important public positions with substantial authority over policy, operations or the use of allocation of government-owned resources, such as senior government officials, senior executive of government corporations, senior politicians, important political party officials, as well as their close family and close associates”;
- people residing in and/or having funds from high-risk countries, including countries “identified by credible sources as having inadequate anti-money laundering standards or representing high-risk for crime and corruption”; and
- people involved in types of “economic or business activities or sectors known to be susceptible to money laundering.”

Clients may also require greater scrutiny as a result of

- information gained from monitoring their activities;
- external inquiries;
- derogatory information, such as negative news reporting; and
- other factors that may expose the bank to reputational risk.

The Wolfsberg principles say that banks should have written policies on the “identification of and follow-up on unusual or suspicious activities,” and should include a definition of what is suspicious, as well as examples of such activity. They recommend a sufficient monitoring system that uses the private banker’s knowledge of the types of activity that would be suspicious for particular clients. They also outline mechanisms that can be used to identify suspicious activity, including meetings, discussions and in-country visits with clients and steps that should be taken when suspicious activity is detected.

The Principles also addressed

- reporting to management of money laundering issues;
- AML training;
- retention of relevant documents;
- deviations from policy; and
- creation of an anti-money laundering department and an AML policy.

One of the key revisions made in May 2001 related to the prohibition of the use of internal nonclient accounts (sometimes referred to as concentration accounts) to keep clients from being linked to the movement of funds on their behalf. It stated that banks should forbid the use of such internal accounts in a manner that would prevent officials from appropriately monitoring movements of client funds.

The Wolfsberg Group also issued guidelines in early 2002 on the suppression of the financing of terrorism, outlining the roles of financial institutions in the fight against money laundering and terrorism financing.

The Wolfsberg recommendations included

- providing official lists of suspected terrorists on a globally coordinated basis by relevant authorities;
- including adequate information in the lists to help institutions search customer databases efficiently;
- providing prompt feedback to institutions following circulation of the official lists;
- providing information on the manner, means and methods used by terrorists;
- developing government guidelines for business sectors and activities identified as high-risk for terrorism financing;
- developing uniform global formats for funds transfers that assist in the detection of terrorism financing;
- protecting financial institutions with safe harbor immunity to encourage them to share information and to report to authorities; and

- performing enhanced due diligence for “business relationships with remittance businesses, exchange houses, casas de cambio, bureaux de change and money transfer agents” and other high-risk customers or those in high-risk sectors and activities “such as underground banking businesses or alternative remittance systems.”

In 2002, Wolfsberg issued guidelines on anti-money laundering principles for correspondent banking that outlined steps financial institutions should take to combat money laundering and terrorism financing through correspondent banking. Correspondent accounts are established by one financial institution with another financial institution to hold deposits, make payments on its behalf and process other transactions. (*See Chapter 2 for more.*)

The guidelines were updated in 2014 to highlight that the principles were intended to address the risks associated with foreign correspondent relationships not domestic. These guidelines extend to all correspondent banking relationships an institution maintains or establishes including where the correspondent banking client is an affiliate, subsidiary or branch of that institution.

Some of the more notable recommendations are as follows.

- Due diligence should be risk-based and on an ongoing basis, depending on the location, type of business, ownership, customer base, regulatory status and AML controls of the correspondent banking client or business. It is recommended that the following elements be considered when conducting due diligence.
  - Geographic risk
  - Branches, subsidiaries and affiliates of correspondent banking clients and of the institution
  - Ownership and management structures of the correspondent banking client
  - Client’s customer base and business
  - Client’s products and services
  - Client’s regulatory status and history
  - Client’s anti-money laundering controls
  - Client’s dealings with shell banks
  - Visits to the client’s business
  - Enhanced due diligence regarding the involvement of PEPs with the correspondent banking client and downstream correspondent (nested) relationships the correspondent provides
  - The principles should be part of a financial institution’s larger AML program including anti-bribery and corruption, fraud and evasion of sanctions

The Wolfsberg Group began collaborating with the Banker’s Almanac in 2004 to develop the International Due Diligence Repository. Details in the Repository include copies of company bylaws, relevant licenses, extracts from commercial registers or certificates of incorporation, the most recent annual reports, information about shareholders with stakes of more than 5 percent, biographies of board members and senior management and information about each financial institution’s AML policies and procedures. The initiative is a move toward standardizing due diligence information,

which in itself provides a potential cost-saving in time spent seeking information from a variety of sources. Since its launch, the Banker's Almanac has added further functionality to the Repository with the inclusion of an alert service that updates users with any changes to documents or status of an institution.

The group released *Monitoring, Screening and Searching Wolfsberg Statement* in September 2003 and further updated in 2009 to provide further guidance on “the design, implementation and ongoing maintenance of transaction monitoring frameworks for real-time screening, transaction monitoring and retroactive searches.” This document discussed the need for appropriate monitoring of transactions and customers to identify potentially unusual or suspicious activity and transactions and for reporting such to competent authorities. In particular, it covered issues related to the development of risk-based processes for monitoring, screening and searching transactions and customers.

All of the Group's publications can be found online at [www.wolfsberg-principles.com/standards.html](http://www.wolfsberg-principles.com/standards.html).

As of June 2016, the Wolfsberg Standards listed on the website were as follows.

- Wolfsberg CB Principles 2014
- Wolfsberg Group MIPS Paper, 2014
- Wolfsberg Private Banking Principles, May 2012
- Wolfsberg Guidance on Prepaid & Stored Value Cards Oct 14, 2011
- Wolfsberg Anti-Corruption Guidance (2011)
- Statement on the publication of the Wolfsberg Anti-Corruption Guidance August 2011
- The Wolfsberg Trade Finance Principles (2011)
- Wolfsberg Monitoring Screening Searching Paper—November 9, 2009
- Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities—May 2009
- Wolfsberg Group, Clearing House Statement on Payment Message Standards—April 2007
- Wolfsberg Group, Notification for Correspondent Bank Customers—April 2007
- Wolfsberg Statement—Guidance on a Risk Based Approach for Managing Money Laundering Risks—March 2006
- Wolfsberg Statement—Anti-Money Laundering Guidance for Mutual Funds and Other Pooled Investment Vehicles—March 2006
- Wolfsberg Statement on The Suppression of the Financing of Terrorism—January 2002

## The World Bank and the International Monetary Fund

---

The International Monetary Fund (IMF) and the World Bank have supported the efforts of FATF in addressing the resistance of certain nations to joining the international battle against money laundering. Since 2001, the two institutions have required countries that benefit from their financial and structural assistance programs to have effective money laundering controls.

In an April 2000 joint policy paper called, “Enhancing Contributions To Combating Money Laundering,” the two organizations detailed the steps that they would take to strengthen the global assault on money laundering.

In September 2001, the IMF and the World Bank started to fully integrate the battle against money laundering and other financial crimes into its surveillance exercises and programs. That month, the International Monetary and Financial Committee (IMFC), the advisers to the IMF’s board of governors, issued a communiqué that said it would “explore incorporating work on financial abuse, particularly with respect to international efforts to fight against money laundering, into its various activities, as relevant and appropriate.”

In February 2001, the IMFC, along with the IMF and the World Bank, issued *Financial System Abuse, Financial Crime, and Money Laundering*, which explored how the institutions could “play ... role[s] in protecting the integrity of the international financial system from abuse” through use of their influence to promote national anti-corruption programs.

Since then, the IMF and the World Bank have become more active in combating money laundering by

- concentrating on money laundering over other forms of financial abuse;
- helping to strengthen financial supervision and regulation in countries;
- more closely interacting with the Organization for Economic Co-operation and Development (OECD) and the Basel Committee on Banking Supervision; and
- insisting on the application of international AML standards in countries that ask for financial assistance.

In a joint meeting in April 2004, the two bodies agreed to permanently adopt their pilot program that assesses a nation’s compliance with international AML and anti-terrorist financing standards. The program put an end to FATF’s practice of publicizing noncooperative countries and territories (NCCTs).

The World Bank and the IMF established a collaborative framework with FATF for conducting comprehensive assessments using a single global methodology of countries’ compliance with FATF’s 40 Recommendations. The assessments are carried out as part of the Financial Sector Assessment Program and result in the Report on Observance of Standards and Codes (ROSCs). ROSCs summarize the extent to which countries observe 12 areas and associated standards for their operational work of the Fund and the World Bank. The 12 areas include: accounting; auditing; AML/CFT; banking supervision; corporate governance; data dissemination; fiscal transparency; insolvency and creditor rights; insurance supervision; monetary and financial policy transparency; payments systems; and securities regulation. The ROSCs are prepared and published at the request of the member country and summarize a countries’ observance of the standards. The Reports are used to help sharpen the

institutions' policy discussions with national authorities and in the private sector, including by rating agencies, for risk assessment purposes. Updates to the ROSCs are produced regularly, however, new reports are prepared and published every several years.

In 2002, the World Bank and the IMF developed the *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* in an effort to provide practical steps for countries implementing AML/CFT regimes in accordance with international standards. A Second Edition and Supplement on Special Recommendation IX was published in 2006. The guide describes the global problem of money laundering and terrorist financing on the development agenda of individual countries and across regions. It explains the basic elements required to build an effective AML/CFT legal and institutional framework and summarizes the role of the World Bank and the IMF in those efforts.

Group	What is It?	Important Documents
<b>Financial Action Task Force on Money Laundering</b>	<ul style="list-style-type: none"> <li>• Intergovernmental body with 34 member countries and two international organizations</li> <li>• Sets money laundering and terrorist financing standards</li> </ul>	<ul style="list-style-type: none"> <li>• 40 Recommendations on Money Laundering and Terrorist Financing (Last updated February 2012)</li> </ul>
<b>Basel Committee on Banking Supervision</b>	<ul style="list-style-type: none"> <li>• Established by the central bank governors of the G-10</li> <li>• Promotes sound supervisory standards worldwide</li> </ul>	<ul style="list-style-type: none"> <li>• Customer Due Diligence for Banks Paper (2001)</li> <li>• Sharing of Financial Records Between Jurisdictions in Connection With the Fight Against Terrorist Financing (2002)</li> <li>• General Guide to Account Opening and Customer Identification (2003, updated 2016)</li> <li>• Consolidated KYC Risk Management Paper (2004, updated 2016)</li> </ul>
<b>European Union</b>	<ul style="list-style-type: none"> <li>• A politico-economic union of 28 member states that are located primarily in Europe</li> <li>• Issues AML/CFT directives regarding legislation that member states must issue to prevent their domestic financial systems being used for money laundering and terrorist financing</li> </ul>	<ul style="list-style-type: none"> <li>• First EU Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering (1991)</li> <li>• Second Directive (2001)</li> <li>• Third Directive (2005)</li> <li>• Fourth Directive (2015)</li> </ul>

Group	What is It?	Important Documents
<b>Wolfsberg Group</b>	<ul style="list-style-type: none"> <li>• Association of 13 global banks</li> <li>• Aims to develop standards on money laundering controls for banks</li> </ul>	<ul style="list-style-type: none"> <li>• Wolfsberg Anti-Money Laundering Principles for Private Banking (last updated 2002)</li> <li>• The Suppression of the Financing of Terrorism Guidelines (2002)</li> <li>• Anti-Money Laundering Principles for Correspondent Banking (2002)</li> </ul>
<b>APG, CFATF, EAG, GABAC, GIABA, GAFILAT, MENAFATF, MONEYVAL, ESAALMG</b>	<ul style="list-style-type: none"> <li>• FATF-style regional bodies that have similar form and functions to those of FATF.</li> <li>• Provide input to FATF on standards and typologies.</li> </ul>	<ul style="list-style-type: none"> <li>• Typologies and so on</li> </ul>
<b>Egmont Group</b>	<ul style="list-style-type: none"> <li>• Informal networking group of financial intelligence units</li> </ul>	<ul style="list-style-type: none"> <li>• Statement of Purpose (last updated 2004)</li> <li>• Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (2001)</li> <li>• Best Practices for the Exchange of Information Between Financial Intelligence Units (2004)</li> </ul>
<b>CICAD</b>	<ul style="list-style-type: none"> <li>• Commission within the Organization of American States that deals with drug-related issues, including money laundering</li> </ul>	<ul style="list-style-type: none"> <li>• Model Regulations</li> </ul>
<b>World Bank and International Monetary Fund</b>	<ul style="list-style-type: none"> <li>• These organizations work together and in conjunction with FATF to encourage countries to have adequate anti-money laundering laws and to review anti-money laundering laws and procedures of FATF member countries.</li> </ul>	<ul style="list-style-type: none"> <li>• Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: A Manual for Countries to Establish and Improve Their Institutional Framework 2002 (revised 2007).</li> </ul>

## Key U.S. Legislative and Regulatory Initiatives Applied to Transactions Internationally

---

This section contains an overview of the principal elements of U. S. laws related to money laundering and terrorism financing that bear on international transactions and jurisdictions.

### USA PATRIOT Act

---

Motivated by the attacks of September 11, 2001, and the urgent need to decipher and disable mechanisms that finance terrorism, the U.S. Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) in October 2001 to strengthen money laundering laws and the Bank Secrecy Act (BSA) to levels unseen since the original passage of the BSA in 1970 and the Money Laundering Control Act of 1986 (Public Law 99-570), the world's first law to criminalize money laundering.

Title III of the USA PATRIOT Act (U.S. Public Law 107-56), entitled, “The International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001,” contains most, though not all, of the anti-money laundering-related provisions in this diverse law. The purpose of Title III is “increasing the strength of U.S. measures to prevent, detect, and prosecute international money laundering and the financing of terrorism, to provide a national mandate for subjecting to special scrutiny foreign jurisdictions, financial institutions operating outside the United States, and classes of international transactions or types of accounts that pose particular opportunities for criminal abuse, and to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities.”

As noted in its purpose, the USA PATRIOT Act has implications for U.S. institutions and non-U.S. institutions that do business in the United States. It is important to note that the regulations issued under the USA PATRIOT Act by the U.S. Treasury Department provide the detailed requirements that financial institutions must follow to comply with the provisions of the Act. These regulations are compiled in 31 Code of Federal Regulation Chapter X.

Key provisions of the USA PATRIOT Act stem from the premise that international access points to the U.S. financial system must be controlled. Thus, the law covers a wide range of anti-money laundering and terrorism-financing provisions affecting foreign businesses. These include the following.

#### **Section 311: Special Measures for Primary Money Laundering Concerns (31 U.S.C. 5318A).**

This section provides the U.S. Treasury Department with the authority to apply graduated, proportionate measures against a foreign jurisdiction, a foreign financial institution, a type of international transaction or a type of account that the Treasury Secretary determines to be a “primary money laundering concern.” By designating a country or a financial institution as a primary money laundering concern, the U.S. government can force U.S. banks to halt many of their financial dealings with the designee. Once identified, the Treasury Department can require U.S. financial institutions to follow any or all of the following five special measures.

1. Keep records and/or file reports on certain financial transactions, including a description of the transactions, the identities and addresses of the participants in the transactions and the identities of the beneficial owners of the funds involved.
2. Obtain information on the beneficial ownership of any account opened or maintained in the United States by a foreign person or a foreign person's representative.
3. Identify and obtain information about customers who are permitted to use, or whose transactions are routed through, a foreign bank's payable-through account.
4. Identify and obtain information about customers permitted to use, or whose transactions are routed through, a foreign bank's correspondent account.
5. Close certain payable-through or correspondent accounts.

To ensure that all relevant factors are considered, the Treasury Secretary must consult with the Secretary of State and the Attorney General before designating a jurisdiction, institution or a particular type of transaction or account as a primary money laundering concern.

Section 311 actions are distinct from designations brought by Treasury's Office of Foreign Assets Control (OFAC), which are applied more broadly and can also trigger asset freezing obligations.

**Section 312: Correspondent and Private Banking Accounts (31 U.S.C. 5318(i)).** Requires due diligence and, in certain situations, enhanced due diligence for foreign correspondent accounts (which includes virtually all account relationships that institutions can have with a foreign financial institution) and private banking for non-U.S. people.

The correspondent banking portions of the rule apply to U.S. banks, credit unions, thrift institutions, trust banks, broker-dealers, futures commission merchants and introducing brokers in commodities and mutual funds and U.S.-based agencies and branches of foreign banks.

Foreign financial institutions covered by the rule include foreign banks, foreign branches of U.S. banks, foreign businesses that would be considered broker-dealers, futures commission merchants, introducing brokers in commodities, mutual funds if they operate in the United States and money transmitters or currency exchangers organized in a foreign country.

The due diligence program must be "appropriate, specific and risk-based," and, where necessary, include enhanced policies, procedures and controls reasonably designed to identify and report suspected money laundering in a correspondent account maintained in the United States. This due diligence program must also be included in the institution's anti-money laundering program.

The due diligence program must address three measures.

1. Determining whether enhanced due diligence is necessary
2. Assessing the money laundering risk presented by the correspondent account
3. Applying risk-based procedures and controls reasonably designed to detect and report suspected money laundering

Pursuant to the implementing regulation, enhanced due diligence procedures must be applied to a correspondent account established for a foreign bank operating under

- an offshore banking license;
- a license issued by a foreign country designated as noncooperative by an international organization, with which designation the Treasury Secretary agrees; and
- a license issued by a foreign country that has been designated by the U.S. Secretary of the Treasury as warranting special measures pursuant to Section 311 of the USA PATRIOT Act.

The enhanced due diligence that must be implemented in these situations includes

- conducting enhanced scrutiny for possible money laundering and suspicious transactions, including
  - obtaining information relating to the foreign bank's AML program,
  - monitoring transactions in and out of the correspondent account in a manner reasonably designed to detect possible money laundering and suspicious activity, and
  - obtaining information about the correspondent account that is being used as a payable-through account;
- determining whether the correspondent account is being used by other foreign banks that have a correspondent relationship with the foreign bank for which the correspondent account was established and taking reasonable steps to assess and mitigate the money laundering risks associated with such accounts; and
- determining, for any such foreign bank whose shares are not publicly traded, the identity of each of the owners of the foreign bank with the power to vote 10 percent or more of any class of securities of the bank and the nature and extent of the ownership interest of each such owner.

The private banking portions of the rule apply to the same institutions covered by the correspondent banking provisions. Such institutions must maintain a due diligence program for private banking accounts and must conduct enhanced scrutiny of private banking accounts maintained for senior foreign political figures, their immediate family and their close associates.

Under the rule, a private banking account is defined as (a) an account with a minimum aggregate deposit of \$1 million, (b) for one or more non-U.S. people and (c) which is assigned to a bank employee acting as a liaison with the non-U.S. person.

For covered private banking accounts, U.S. institutions must take reasonable steps to

- ascertain the identity of all nominal and beneficial owners of the accounts;
- ascertain whether any such owner is a senior foreign political figure;
- ascertain the source of the funds in the account and the purpose and expected use of the account; and
- monitor the account to ensure the activity in the account is consistent with the information provided as to the source of funds and the purpose and expected use of the account, as needed, to guard against money laundering and to report any suspected money laundering or suspicious activity.

In ascertaining whether an account owner is a senior foreign political figure, the institution must take reasonable steps to determine if the person is a “current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government.” The definition also covers officials of foreign political parties and government-owned commercial enterprises. The definition includes immediate family members and persons who are “widely and publicly known” to be close associates.

An institution that maintains accounts for these individuals must conduct enhanced scrutiny that is reasonably designed to detect if the funds “may involve the proceeds of foreign corruption,” which includes any asset or property obtained “through misappropriation, theft or embezzlement of public funds, the unlawful conversion of property of a foreign government, or ... bribery or extortion.”

**Section 313: Prohibition on correspondent accounts for foreign shell banks (31 U.S.C. 5318(j)).** Prohibits U.S. banks and securities brokers and dealers from maintaining correspondent accounts for foreign, unregulated shell banks that have no physical presence anywhere. The term physical presence is defined as a place of business that is maintained by a foreign bank located at a fixed address (as opposed to solely an electronic address) where: it is authorized to conduct banking activities; employs one or more individuals on a full-time basis at that location; maintains operating records at that location; and is subject to inspection by the banking authority which licensed it at that location. The term *shell bank* does not include a bank that is a regulated affiliate of a bank that maintains a physical presence.

The section also requires financial institutions to take reasonable steps to ensure that foreign banks with correspondent accounts do not themselves permit access to such accounts by foreign shell banks. Banks and securities brokers are permitted to use a certification form to comply with the rule. That process requires the foreign banks to certify at least once every 3 years that they are not themselves shell banks and that they do not permit shell banks access to the U.S. correspondent account through a nested correspondent relationship.

**Sections 314 (A) and 314(B): Help “law enforcement identify, disrupt, and prevent terrorist acts and money laundering activities by encouraging further cooperation among law enforcement, regulators, and financial institutions to share information regarding those suspected of being involved in terrorism or money laundering.”**

- **Section 314(a):** FinCEN’s regulations under Section 314(a) enable U.S. federal, state, local and foreign (European Union) law enforcement agencies, through FinCEN, to reach out to more than 43,000 points of contact at more than 22,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering. To obtain documents from a financial institution that has reported a match of a subject, a law enforcement agency must meet the legal standards that apply to the particular investigative tool that it chooses to use to obtain the documents.
- **Section 314(b):** Provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities. 314(b) information sharing is a voluntary program. Entities that may participate in 314(b) include U.S. financial institutions

subject to an anti-money laundering program requirement under FinCEN regulations and any association of such financial institutions. This currently includes the following types of U.S. financial institutions.

- Banks
- Casinos and card clubs
- Money services businesses
- Brokers or dealers in securities
- Mutual funds
- Insurance companies
- Futures commission merchants and introducing brokers in commodities
- Dealers in precious metals, precious stones or jewels
- Operators of credit card systems
- Loan or finance companies

**Section 319(a): Forfeiture from U.S. Correspondent Account (18 U.S.C. 981(k)).** In situations where funds have been deposited with a foreign bank, this section permits the U.S. government to seize funds in the same amount from a correspondent bank account in the United States that has been opened and maintained for the foreign bank. The U.S. government is not required to trace the funds, because they are deemed to have been deposited into the correspondent account. However, the owner of the funds may contest the seizure order.

**Section 319(b): Records relating to Correspondent Accounts for Foreign Banks (31 U.S.C. 5318(k)).** Allows the appropriate federal banking agency to require a financial institution to produce within 120 hours (5 days) records or information related to the institution's AML compliance or related to a customer of the institution or any account opened, maintained, administered or managed in the United States by the financial institution.

The section also allows the Secretary of the Treasury or the Attorney General to subpoena records of a foreign bank that maintains a correspondent account in the United States. The subpoena can request any records relating to the account, including records located outside the United States. If the foreign bank fails to comply with or fails to contest the subpoena, the Secretary or the Attorney General can order the U.S. financial institution to close the correspondent account within 10 days of receipt of such an order.

Additionally, the section also requires foreign banks to designate a registered agent in the United States to accept service of subpoenas pursuant to this section. Furthermore, U.S. banks and securities brokers and dealers that maintain correspondent accounts for foreign banks must keep records of the identity of the 25 percent owners of the foreign bank, unless it is publicly traded, as well as the name of the correspondent bank's registered agent in the U.S.

This information is generally collected on the certification form used to comply with Section 313 and must be updated at least every 3 years or more frequently, if the information is no longer correct.

## The Reach of the U.S. Criminal Money Laundering and Civil Forfeiture Laws

---

The Money Laundering Control Act of 1986, the first criminal money laundering law of the United States, is a powerful legal weapon that may be used if the property involved in the financial transaction at issue represents the proceeds of at least one designated underlying crime—a “specified unlawful activity” (SUA). SUAs include virtually every U.S. crime that produces economic advantage, including aircraft piracy, wire fraud, bank fraud, copyright infringement, embezzlement, export violations, illegal gambling, narcotics offenses, racketeering and even some environmental crimes. (18 USC 1956 and 1957.)

This money laundering law also reaches foreign individuals and foreign financial institutions if the financial transaction occurs in whole or in part in the United States or, if the foreign financial institution maintains a bank account at a U.S. financial institution.

Although the prosecution must prove the existence of an SUA’s proceeds, it need not prove that the accused knew the exact source of the funds. The prosecution must prove only that the defendant knew that the funds came “from some form ... of activity that constitutes a felony under state, federal, or foreign law, regardless of whether or not such activity” is an SUA (18 USC 1956(c)(1)). Courts have often ruled that willful blindness, which has been defined as “the deliberate avoidance of knowledge of the facts,” is the equivalent of actual knowledge. Willful blindness may be proven by the circumstances surrounding the transaction and the defendant’s conduct.

Section 319(a) of the USA PATRIOT Act, discussed above, greatly strengthened the forfeiture powers over the funds of foreign persons and institutions. If the funds the United States pursues are deposited in a foreign bank that keeps an interbank account at a U.S. bank, the United States may bring a case to forfeit the crime-tainted funds in the U.S. account.

### *Case Study*

In April 2012, the U.S. Attorney’s Office for the Southern District of New York seized \$16.3 million held in Wegelin & Co.’s U.S. correspondent account with UBS AG in Stamford, Connecticut. Founded in 1741, Wegelin was Switzerland’s oldest bank and specialized in private banking, asset management and other services to clients worldwide, including U.S. taxpayers. The civil forfeiture complaint alleged that Wegelin used its correspondent accounts to assist U.S. taxpayers to evade U.S. tax authorities. By 2010, Wegelin held approximately \$1.5 billion in undeclared U.S. taxpayer funds. In January 2013, after pleading guilty to one count of conspiracy to defraud the IRS, file false federal income tax returns and evade federal income taxes from 2000 through 2011, the bank was sentenced to pay the United States approximately \$58 million. This sentence, combined with the April 2012 civil forfeiture, amounted to a total recovery of approximately \$74 million.

## Office of Foreign Assets Control

---

In addition to these laws and regulations, financial institutions and businesses in other countries must recognize the extraterritorial reach of regulations enforced by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC).

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and to freeze foreign assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates that are multilateral in scope and involve close cooperation with allied governments.

OFAC sanction programs prohibit transactions and require the blocking of assets of persons and organizations that appear on one of a series of lists that OFAC issues periodically. OFAC has the power to impose significant penalties on those who are found to be in violation of the blocking orders within each of the sanction programs.

All U.S. people must comply with OFAC regulations, including: all U.S. citizens and permanent resident aliens, regardless of where they are located; all people and entities within the United States and all U.S.-incorporated entities and their foreign branches. In the case of certain programs, such as those regarding North Korea, Syria and Cuba, all foreign subsidiaries owned or controlled by companies also must comply. Please note, however, that the United States is in the process of amending its regulations on Cuban sanctions programs. Certain programs also require foreign persons in possession of U.S.-origin goods to comply.

### Case Study

In 2014, OFAC reached a record \$963 million settlement with BNP Paribas SA (BNPP), Paris, France, following a \$8.9 billion penalty imposed for apparent violations of U.S. sanctions regulations. The settlement resolved OFAC's investigation into BNPP's systemic practice of concealing, removing, omitting or obscuring references to information about U.S.-sanctioned parties in almost 4,000 financial transactions routed to or through U.S. banks between 2005 and 2012 in apparent violation of U.S. sanctions involving Sudan, Iran, Cuba and Burma. BNPP's methods for processing sanctions-related payments to or through the United States included removing references to sanctioned parties, replacing sanctioned parties with BNPP's name or a code word or otherwise structuring the payments in a matter that did not identify the involvement of the sanctioned parties in the transactions.

**NOTES:**

[illegible]





# Chapter 3

## Anti-Money Laundering/Counter-Terrorist Financing Compliance Programs

An anti-money laundering/counter-terrorist financing program (AML/CFT program) is an essential component of a financial institution's compliance regime. The primary goal of an AML/CFT program is to protect the organization against money laundering, terrorist financing and other financial crimes and to ensure that the organization is in full compliance with relevant laws and regulations. For that reason, designing, structuring and implementing these programs should be the top priorities of any financial institution.

An AML/CFT program should be risk-based. Certain aspects of a financial institution's business will pose greater money laundering risks than others and will require additional controls to mitigate those risks, while others will present a minimal risk and will not need the same level of attention.

Depending on the size of the organization, the anti-money laundering function may be managed as a dedicated/stand-alone department, integrated into other corporate departments such as the legal department or may be performed by people who have other compliance duties. Regardless of the size of the organization, the program should have an enterprise-wide view of AML/CFT efforts.

The AML/CFT program should establish minimum standards for the enterprise that are reasonably designed to comply with all applicable laws and regulations. It may be supplemented by the policies and procedures of various lines of business or legal entities that address specific areas, such as private banking, trade finance, cash handling, institutional banking, wealth management or investigations. Compliance programs should also include corporate governance and overall management of money laundering and terrorist financing risks.

Before designing an AML/CFT program, it is imperative to understand what is required of a financial institution, its employees and customers by the laws and regulations of all of the jurisdictions where the financial institution is doing business and where its customers are located. The financial institution's internal policies and risk management standards related to the business must also be taken into consideration. Anyone needing advice on the complexities of AML/CFT legislation before developing an AML/CFT program should consult a competent advisor, even if it means seeking external assistance.

In this section, we will discuss what to consider when designing a compliance program; how to assess risk; how to identify, manage, document and follow up on suspicious activities; how to know your customer and employee; how to audit your program effectively; and what you need to know about training and screening employees.

## Assessing AML/CFT Risk

---

### Introduction

---

Understanding what is legally required of your institution, employees and customers is essential to a successful program. It is also important to understand the expectations of the relevant AML/CFT regulators and/or supervisory authorities.

The Financial Action Task Force (FATF), along with numerous member countries, such as the UK and United States, urge risk-based controls. Per FATF, there are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced customer due diligence (CDD) measures have to be taken.

A risk-based approach requires financial institutions to have systems and controls that are commensurate with the specific risks of money laundering and terrorist financing facing them. Assessing this risk is, therefore, one of the most important steps in creating a good AML/CFT compliance program. As money laundering risks increase, stronger controls are necessary. However, all categories of risk—whether low, medium or high—must be identified and mitigated by the application of controls, such as verification of customer identity, customer due diligence policies, suspicious activity monitoring and economic sanctions screening.

The majority of governments around the world believe that the risk-based approach is preferable to a more prescriptive approach in the area of AML/CFT because it is more

- **flexible** because as money laundering and terrorist financing risks vary across jurisdictions, customers, products and delivery channels and over time;
- **effective** because as companies are better equipped than legislators to effectively assess and mitigate the particular money laundering and terrorist financing risks they face; and
- **proportionate** because a risk-based approach promotes a common sense and intelligent approach to fighting money laundering and terrorist financing as opposed to a check-the-box approach. It also allows firms to minimize the adverse impact of anti-money laundering procedures on their low-risk customers.

The theory is that no financial institution can reasonably be expected to detect all wrongdoing by customers, including money laundering. But if a financial institution develops systems and procedures to detect, monitor and report the riskier customers and transactions, it will increase its chances of staying out of harm's way from criminals and from government sanctions and penalties.

The risks a financial institution faces depend on many factors, including the geographical regions involved, customer types and the products and services offered.

When assessing risk, FATF recommends considering

- customer risk factors such as nonresident customers, cash-intensive businesses, complex ownership structure of a company and companies with bearer shares;
- country or geographic risks such as countries with inadequate AML/CFT systems, countries subject to sanctions or embargos, countries involved with funding or supporting of terrorist activities or those with significant levels of corruption; and
- product, service, transaction or delivery channel risk factors such as private banking, anonymous transactions and payments received from unknown third parties.

Although not necessarily mandated by AML/CFT legislation in various jurisdictions, many organizations find it valuable to develop money laundering/terrorist financing (ML/TF) risk models that assess risk at the enterprise level, with the customer element providing for ML/TF risk assessments at the customer type level (e.g., individual, company, trust) and also providing capability for the specific customer level (i.e., an ML/TF risk assessment of the customer's entire relationship with the organization). Moreover, some jurisdictions also seek a separate sanctions assessment for reporting entities.

---

## Maintaining an AML/CFT Risk Model

---

A risk-based approach seeks to identify, manage and analyze AML/CFT risk in order to design and effectively implement appropriate controls. As such, it is critical that risk ratings accurately reflect the risks present, provide meaningful assessments that lead to practical steps to mitigate the risks, are periodically reviewed and, when necessary, are updated.

A risk-based analysis should include appropriate inherent and residual risks at the country, sectoral, legal entity and business relationship level, among others. As a result of this analysis, the financial institution should develop a thorough understanding of the inherent risks in its customer base, products, delivery channels and services offered (including proposed new services) and the jurisdictions within which it or its customers do business. This understanding should be based on operational, transaction and other internal information collected by the institution, as well as external sources.

In identifying all relevant ML/TF risks, all relevant information must be taken into account. This usually requires expert input from the business lines, risk management, compliance and legal units together with advice from external experts where necessary. In particular, new business products or services should be evaluated for money laundering and sanctions vulnerabilities with appropriate controls implemented before launching them into the market. There is also a growing body of publicly available helpful guidance on ML/TF risk assessments that should be taken into consideration. Such guidance is regularly published by FATF, regional FATF-styled bodies, regulatory agencies, other institutions such as the United Nations Office on Drugs and Crime (UNODC), the International Monetary Fund (IMF), the World Bank and jurisdiction-specific information, guidance and advisories.

Risk is dynamic and needs to be continuously managed. It should also be noted that the environment in which each organization operates is subject to continual change. Externally, the political changes of a jurisdiction or whether economic sanctions are imposed or removed may impact a country-risk

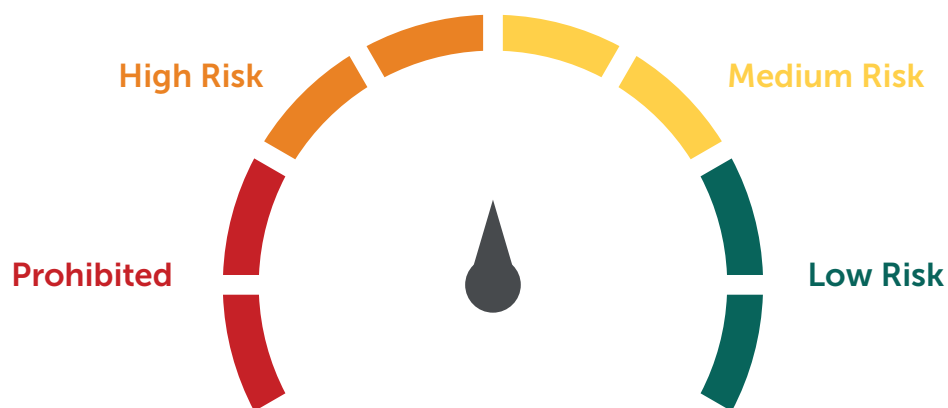
rating. Internally, organizations respond to market and customer demands by introducing new products and services and implementing new delivery systems. The combination of these changes makes it critical that the ML/TF risk model is subject to regular review. In some countries, there is a legislative obligation for such reviews to be undertaken on a regular basis—usually annually or when new products, delivery channels or customer types are introduced.

## Understanding AML/CFT Risk

AML/CFT risk categories can be broken down into the following levels.

- **Prohibited:** The institution will not tolerate any dealings of any kind given the risk. This category could include transactions with countries subject to economic sanctions or designated as state sponsors of terrorism, such as those on the United Nations or Office of Foreign Assets Control lists.
- **High-risk:** The risks here are significant, but are not necessarily prohibited. To mitigate the heightened risk presented, the financial institution should apply more stringent controls to reduce the ML/TF risk, such as conducting enhanced due diligence and more rigorous transaction monitoring. Countries that maintain a reputation for corruption or drug trafficking are generally considered high-risk. High-risk customers may include politically exposed persons (PEPs) or certain types of money services businesses or cash-intensive businesses; high-risk products and services may include correspondent banking and private banking.
- **Medium Risk:** Medium risks merit additional scrutiny, but do not rise to the level of high-risk. For example, a retail business that accepts low to moderate levels of cash, but is not considered cash-intensive.
- **Low Risk:** This represents the baseline risk of money laundering. Typically, low risk indicates normal, expected activity.

### AML/CFT Risk



## AML/CFT Risk Scoring

A risk-scoring model uses numeric values to determine the category of risk (geography, customer type and products and services) and the overall customer risk. For example, each category could be given a score between 1 and 10, with 10 being the riskiest. The individual categories could be scored with 1–3 being standard risk, 4–8 being medium risk and 9–10 being high-risk. Such a model is particularly helpful when looking at product risk because it will help determine appropriate controls for the products.

The three categories are then combined to give a composite score. A simple model would just add the totals from the categories, which would yield a score between 3 and 30. The model can be made more complex by weighting each of the factors differently, such as putting more emphasis on the type of customer, as opposed to the product or country. The model can be made even more sophisticated by, for instance, creating combinations of factors that will determine the overall rating. The degree of complexity is up to the institution; the more complex, the more likely the rating will reflect the customer's overall risk.

In a simple three-element model like the one first described above, care must be taken to not inadvertently discount any element that is an outlier from the other elements. For example, if each element has a risk score of 3, then the composite or aggregate score will be 9. However, if two of the three elements have a score of 1 and the other has a score of 7, then the composite risk score is also 9. In this case, there is a need to identify how and in what manner the element scoring 7 should be mitigated. This could mean implementing a more rigorous control or introducing restrictions.

It is important to understand that when the categories are combined the customer's risk picture becomes clearer. For instance, when you combine a product with a customer type, the combination can radically change the level of risk. For example, you have a small, foreign, private company that you don't have much information about seeking to open a checking account with online wire transfer capabilities. That customer's ability to rapidly transfer funds raises its risk level. The customer may also have higher risk ratings for geography, customer type and products and services. Another example is you have a publicly listed domestic company listed on a major stock market that wants to establish an employee retirement plan. Public companies must provide a lot to be listed on the major stock market. What is more, retirement plan accounts are not very vulnerable to money laundering. As a result, this customer and account will have a much lower risk than the above example of the foreign private company.

The next step is to determine what thresholds to establish for each risk category. The institution should be mindful that high-risk relationships should not represent too large a segment of the population; this is not to say the scores should be adapted to fit the customer portfolio, rather, because high-risk customers truly do need more attention. In addition, if the portfolio is overly weighted toward high-risk the overall risk level in the institution may be too great to support.

Assessing AML/CFT is an ongoing and evolving component of maintaining a compliant AML/CFT program. Evaluating the risk-scoring model and conducting the risk assessment itself may need to be performed annually, every 18 to 24 months, before the launch of a new product or when an acquisition of another financial institution occurs.

Periodically reassessing risk-rating criteria will show if the customers that are scored as higher risk are actually more likely to engage in potentially suspicious activity. If they are not, it may be time to reassess the risk-scoring model.

## **Assessing The Dynamic Risk of Customers**

---

Another critical component of a risk assessment is having a process to reevaluate risks and determine when the customer risk rating should be raised or lowered. Identifying the key factors that should trigger such a reevaluation is essential to efficient allocation of limited resources.

In addition to the initial assessment of the inherent risk of a customer, it is important to consider how a customer's relationship—and risk—with the institution changes over time. Perhaps the most important consideration driving a customer's risk rating is the actual activity that the customer conducts. For example, a student checking account may start out as low risk. But if records show that it is involved in a large number and volume of wires to higher risk jurisdictions, which indicates abnormal behavior for this client type, the risk level for this account may need to be raised. Similarly, a potentially higher risk customer, such as a money services business (MSB) or correspondent bank, may be engaging in exactly the type of activity it indicates it will conduct. This customer may not be as risky as one might think based solely on the inherent risk. And so the low or standard risk student customer based solely on inherent risk may actually present more risk to the institution than the MSB that presents a high inherent risk.

As every financial institution develops transaction history with customers, it should consider modifying the risk rating of the customer, based on

- unusual activity, such as alerts, cases and suspicious transaction report (STR) filings;
- receipt of law enforcement inquiries, such as subpoenas;
- transactions that violate economic sanctions programs; and
- other considerations, such as significant volumes of activity where it would not be expected, such as a domestic charity engaging in large international transactions or businesses engaged in large volumes of cash where this would not normally be expected.

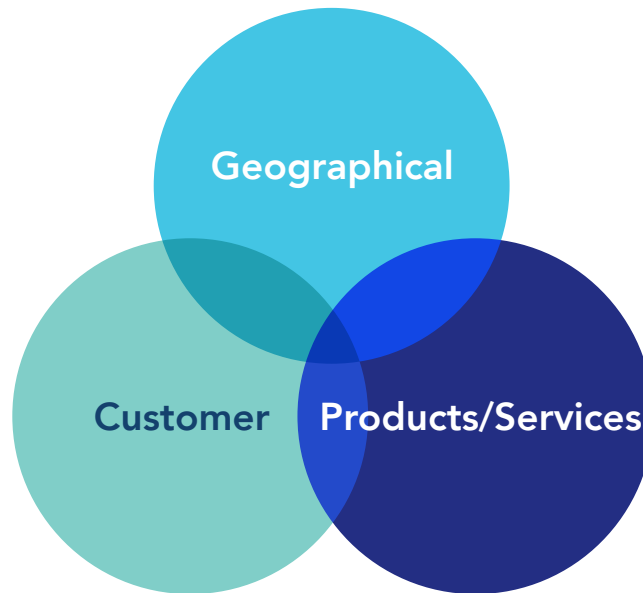
The institution knowledge of the customer based on its activity will better determine the actual risk presented by a customer. As noted elsewhere, higher risk customers, including those whose activity drives a higher risk rating, should be subject to enhanced due diligence (EDD) to mitigate the risk. This EDD might ultimately determine the activity is not suspicious. If so, the customer record should be to reflect a change that explains its activity.

## **AML/CFT Risk Identification**

---

The core of a risk-based approach includes the assessment of risk of a financial institution's customers, geography locations and its products/services. Below is a deeper look into the three important risk factors.

## Risk Types/Factors



### CUSTOMER TYPE

A vital step in a risk assessment is the analysis of the users of the products and services that the institution or business offers. Customer types can include individuals, listed companies, private companies, joint ventures, partnerships and financial institutions; basically anyone who wants to establish a relationship with the financial institution.

Customers who have a history of involvement in criminal activities receive the highest ratings. Political figures, or those in political organizations, also score toward the top of the scale.

Multinational public corporations tend to score lower than private companies because there is much more publicly available information and due diligence conducted on a corporation listed on a major stock exchange. Risks are generally higher if a money launderer can hide behind corporate vehicles, such as trusts, charities, limited liability companies or structures, where it is difficult to identify the beneficial owners of the entities. The risk is even higher if corporations are based in countries with inadequate anti-money laundering requirements or strict corporate secrecy protections.

Supervisory authorities in various countries have stated that some types of customers are inherently high-risk for money laundering. They include the following.

- Banks
- Casinos
- Offshore corporations and banks located in tax/banking havens
- Embassies
- MSBs, including currency exchange houses, money remitters, check cashers

- Virtual currency exchanges
- Car, boat and plane dealerships
- Used-car and truck dealers and machine parts manufacturers;
- Professional service providers (attorneys, accountants, investment brokers and other third parties who act as financial liaisons for their clients)
- Travel agencies
- Broker/dealers in securities
- Jewel, gem and precious metals dealers
- Import/export companies
- Cash-intensive businesses (restaurants, retail stores, parking)

The list above does not represent all industries that could be considered to be high-risk. It is important to note that industry alone does not determine risk. Many other types of businesses not listed could also be used to launder money and many other factors need to be considered.

Implementing a strong screening process when onboarding a customer and throughout the duration of the relationship are key components to identifying high-risk customer types.

#### *Case Study*

In November 2014, the Financial Crimes Enforcement Network (FinCEN) issued a \$300,000 civil money penalty against North Dade Community Development Federal Credit Union in Florida for AML program failures that included a significant number of MSBs in its portfolio. The credit union, with \$4 million in assets and five employees, was banking 56 MSBs located in high-risk jurisdictions in Central America, the Middle East and Mexico, all far outside its field of membership. These MSBs comprised 90 percent of North Dade's total annual revenue and conducted almost \$2 billion worth of transactions. One of the failings noted in the order was a failure to conduct a risk assessment, which may have allowed North Dade to identify these risks. Further, North Dade had relied on one of its clients to conduct the due diligence on these MSBs. This was the same client who introduced the MSBs to the credit union. This increased the risk posed to the credit union because it did not independently assess the vendor's due diligence efforts.

## **GEOGRAPHIC LOCATION**

A crucial step in devising a risk-scoring model involves jurisdictional risk. In what countries or jurisdictions do your individual customers reside and what are the customers' countries of citizenship? Where are your corporate customers headquartered and where do they conduct the majority of their business?

There is no definitive, independent system for assessing the money laundering risks of various territories and countries. Some firms will devise their own methods; others will look to a vendor solution. Whichever course is chosen, it is essential that the risk-rating methodology be documented. In larger organizations, the overall risk-management strategy may require the outputs of the ML/TF risk model to be formally reviewed and endorsed by executive/senior management.

When looking specifically at money laundering risk, the terrorism and sanctions lists published by governments and international organizations can be a useful starting point. These include lists published by the United Kingdom's Financial Conduct Authority (FCA), U.S. Office of Foreign Assets Control (OFAC), the U.S. Financial Crimes Enforcement Network (FinCEN), the European Union (EU), the World Bank, the United Nations Security Council and each local jurisdictions' regulatory and law enforcement agencies, such as the Indonesia National Counter Terrorism Agency (BNPT). A model should also take into account whether the country is a member of FATF or of a FATF-style regional body and has AML/CFT requirements equivalent to international best practices.

Companies might also consider the overall reputation of the countries in question. In some, cash may be a standard medium of exchange. Others may have politically unstable regimes and high levels of public or private sector corruption. Some may have a reputation as bank secrecy havens. Still, others may be widely known to have high levels of internal drug production or to be in drug transit regions. How can one identify such countries?

- The U.S. State Department issues an annual *International Narcotics Control Strategy Report* rating more than 100 countries on their money laundering controls.
- Transparency International publishes a yearly *Corruption Perceptions Index*, which rates more than 100 countries on perceived corruption.
- FATF identifies jurisdictions with weak AML/CFT regimes and issues country-specific Mutual Evaluation Reports.
- In the United States, certain domestic jurisdictions are evaluated based on whether they fall within government-identified higher risk geographic locations such as High Intensity Drug Trafficking Areas (HIDTA) or High Intensity Financial Crime Areas (HIFCA).

Monitoring major news media is also recommended, and care should be taken that all of the country lists are monitored on a regular basis for changes.

## PRODUCTS/SERVICES

An important element of assessing AML/CFT risk is to review new and existing products and services that the institution or business offers to determine how they may be used to launder money or finance terrorism. The compliance officer should be an active participant in project teams identifying appropriate control frameworks for new products and systems.

What products and services does your institution offer that may be vulnerable to money laundering or terrorist financing? Internet accounts? Private banking? Money transmittal services? Stock brokerage services? Annuities? Insurance products? Offshore services? Money orders? Correspondent banking?

This risk rating, based on the type of product the customer seeks, is calculated using a number of product-related factors. Most notably, it depends on the likelihood that the product requested might be used for money laundering or terrorist financing. You probably won't see interest-rate swaps being used to finance terror, but securities may be another matter. Product scoring is not universal because different financial institutions face varying degrees of risk.

Does a particular new or current product or service

- enable significant volumes of transactions to occur rapidly;
- allow the customer to engage in transactions with minimal oversight by the institution;
- afford significant levels of anonymity to the users;
- have an especially high transaction or investment value;
- allow payments to third parties;
- have unusual complexity; or
- require government verification of customer eligibility?

In addition, certain specific banking functions or products are considered high-risk. These include the following.

- Private banking
- Offshore international activity
- Deposit-taking facilities
- Wire transfer and cash-management functions
- Transactions in which the primary beneficiary is undisclosed
- Loan guarantee schemes
- Travelers checks
- Official bank checks
- Money orders
- Foreign exchange transactions
- International remittances
- Payment services such as payment processors; prepaid products, automatic clearing house (ACH)
- Remote deposit capture
- Trade-financing transactions with unusual pricing features
- Payable through accounts (PTAs)

## AML/CFT Program

---

### The Elements of an AML/CFT Program

---

Commonly referred to as the four pillars, the basic elements that must be addressed in an AML/CFT program are

- a system of internal policies, procedures and controls (first line of defense);
- a designated compliance function with a compliance officer (second line of defense);
- an ongoing employee training program; and
- an independent audit function to test the overall effectiveness of the AML program (third line of defense).

Although the customer due diligence (CDD) requirements have traditionally been encompassed in the system of internal controls, FATF has focused particular attention on CDD as a critical means of mitigating AML/CFT risk. Under a 2016 rule, FinCEN established a fifth pillar that requires appropriate risk-based procedures for conducting ongoing CDD, raising the prominence of this critical aspect of AML/CFT programs to its own pillar. These procedures include

- understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile;
- conducting ongoing monitoring to identify and report suspicious transactions; and
- maintaining and updating customer information.

The AML/CFT legislation in a number of countries includes mandatory elements that must be included in an AML/CFT program. Organizations should ensure that all such elements are addressed based on the laws and regulations in the jurisdictions they operate in.

### A System of Internal Policies, Procedures and Controls

---

The establishment and continual development of a financial institution's policies, procedures and controls are foundational to a successful AML/CFT program. Together, these three parts define and support the entire AML/CFT program, and at the same time, act as a blueprint that outlines how an institution is fulfilling its regulatory requirements. All three parts should be designed to mitigate the identified AML/CFT risks and should take into account the applicable AML/CFT laws and regulations that the financial institution must comply with. They should clearly indicate the risk appetite of the business; in other words, what risks the business is prepared to accept and those it is not.

Although these controls are normally applied by the first line of defense (the employees who are responsible for onboarding customers), the next few sections will outline how every employee throughout a financial institution, at all levels of an organization, must contribute to the creation, maintenance and overall success of the AML/CFT program.

For larger financial institutions, there is a critical need to adopt an enterprise-wide approach that allows for consistency in the manner in which the financial institution manages its ML/TF risk. However, there is also a need to accommodate regional and/or business line-specific requirements. For example, enterprise-wide ML/TF risk models in financial institutions that operate in multiple regions and/or countries will need to reflect the local regulatory requirements. This may be achieved by having a different version of the AML/CFT program or by having country-specific addenda to the global AML/CFT program.

### *Case Study*

In December 2012, HSBC Holdings PLC and HSBC Bank USA, N.A. agreed to forfeit \$1.2 billion to several U.S. agencies for, among other things, failure to have an enterprise-wide view of compliance across the global institution. As an example, the headquarters in London were aware of weaknesses in its Mexican operations. The U.S. operations processed many of the transactions for the Mexican operations, but were never informed of the weaknesses in the Mexican operations by anyone within the organization. In another example, non-U.S. operations deliberately withheld information from wire transfers that were sent through the U.S. operations that referenced sanctioned parties. Disputes on how to address these matters were not resolved in a prompt manner, which allowed the problem to continue for years. A strong centralized oversight of the program instead of the localized model in place at the time may have been able to mitigate these weaknesses and potentially avert the issues that resulted in the significant penalties.

Internal AML/CFT policies should be established and approved by executive management and the board of directors and should set the tone for the organization. Although the organization's policy may be a high-level statement of principles, it serves as the basis for procedures and controls that provide details as to how lines of business will achieve compliance with laws and regulations and with the organization's AML/CFT policies.

The standard AML/CFT operating procedures should be drafted at the operational level in the financial institution. These procedures must be modified and updated, as needed, to reflect changes in law and regulation, products and organizational changes. These procedures are more detailed than the corresponding AML/CFT policies; they translate policy into acceptable and workable practices. The procedures also form the basis of an important component of AML/CFT training and for compliance monitoring programs. In addition to policies and procedures, there should also be a process to support and facilitate effective implementation of procedures, and that process should be reviewed and updated regularly.

Although policies and procedures provide important guidance, the AML/CFT program also relies on a variety of internal controls, including management reports and other built-in safeguards that keep the program working. These internal controls should enable the compliance organization to recognize deviations from standard procedures and safety protocols. A matter as simple as requiring a corporate officer's approval or two signatures for transactions that exceed a prescribed amount could be a critical internal control element that, if ignored, seriously weakens an institution's AML/CFT program and attracts unwanted attention from supervisory authorities.

Similarly, a second review and approval of actions considered to be departures from policy could be helpful if subsequent questions arise. Other effective controls use technology, such as account opening systems that force the entry of required information, aggregation systems that detect reportable currency transactions and automated account monitoring programs.

## AML POLICIES, PROCEDURES AND CONTROLS

An AML/CFT compliance program should be in writing and include policies, procedures and controls that are designed to prevent, detect and deter money laundering and terrorist financing, including how the institution will

- identify high-risk operations (products, services, delivery channels, customers and geographic locations); provide for periodic updates to the institution's risk profile and provide for an AML/CFT compliance program tailored to manage risks;
- inform the board of directors (or a committee of the board) and senior management of compliance initiatives, known compliance deficiencies, suspicious transaction reports filed and corrective action taken;
- develop and maintain a system of metrics reporting that provides accurate and timely information on the status of the AML/CFT program, including statistics on key elements of the program, such as the number of transactions monitored, alerts generated, cases created and suspicious transaction reports (STRs) filed;
- assign clear accountability to people for performance of duties under the AML/CFT program;
- provide for program continuity despite changes in management or employee composition or structure;
- meet all regulatory requirements and recommendations for AML/CFT compliance;
- provide for periodic review as well as timely updates to implement changes in regulations (this should be done at least on an annual basis);
- implement risk-based CDD policies, procedures and processes;
- provide for dual controls and segregation of duties;
- comply with all record-keeping requirements, including retention and retrieval of records;
- provide sufficient controls and monitoring systems for the timely detection and reporting of potentially suspicious activity and large transaction reporting. This should also include a procedure for recording the rationale for not reporting activity as a result of the findings of any investigation;
- establish clear accountability lines and responsibilities to ensure that there is appropriate and effective oversight of staff who engage in activities which may pose a greater AML/CFT risk;
- establish training requirements and standards in order to ensure that employees are made aware of and have a working understanding of the procedures to be followed and their relevance to mitigating AML/CFT risks in their departments or areas of responsibilities;
- clearly explain the importance of reporting suspicious activity, including describing how and to whom concerns should be raised, the role of the compliance officer and what the "tipping off" restriction means in practice;
- incorporate into all job descriptions and performance review processes the requirement to comply at all times with anti-money laundering policies and procedures. Noncompliance with these should be dealt with in accordance with existing disciplinary processes;

- develop and implement screening programs to ensure high standards when hiring employees. Implement appropriate disciplinary action for employees who consistently fail to perform in accordance with an AML/CFT framework; and
- develop and implement quality assurance testing programs to assess the effectiveness of the AML/CFT program's implementation and execution of its requirements. This is separate from the independent audit requirement, but serves a similar purpose—to assess the ongoing effectiveness of the program.

The level of sophistication a financial institution needs to maintain concerning its policies, procedures and controls directly correlates to the institution's size, structure, risk and complexity of products, amongst other items. Failures to establish, perform, follow or maintain adequate policies, procedures or controls can lead to severe enforcements against the institution or designated individuals involved.

*Case Study:*

In January 2014, the UK Financial Conduct Authority (FCA) fined Standard Bank PLC (Standard Bank) 7.64 million Euros for multiple failures relating to its AML/CFT policies, procedures and controls. Specifically, the bank failed to adequately address the risk associated with customers who had connections to politically exposed persons (PEPs). According to the FCA, “during the relevant period, Standard Bank had business relationships with 5,339 corporate customers of which 282 were linked to one or more PEPs.” The bank had previously identified the shortcomings in its inability to continually monitor these accounts, but they failed to take adequate steps to resolve the issues. As a result, the FCA indicated that Standard Bank was unable to consistently (1) perform adequate EDD measures prior to establishing new accounts with entities who had connections with PEPs and (2) failed to conduct sufficient ongoing monitoring of existing accounts.

<b>Highlights and Differences between AML/CFT Policies, Procedures and Controls</b>	
<b>Policies</b>	<ul style="list-style-type: none"> <li>• Clear and simple high-level statements that are uniform across the entire organization (sets the tone from the top)</li> <li>• Approved by executive management or the board of directors</li> <li>• Reflects the high-level responsibilities of the stakeholders throughout the organization</li> </ul>
<b>Procedures</b>	<ul style="list-style-type: none"> <li>• Translates the AML/CFT policies into an acceptable and workable practice, tasking the stakeholders with their respective responsibilities.</li> <li>• May be established at the operational (not executive) level of the financial institution. These are the instructions on how an institution wants something done.</li> <li>• Much more detailed than AML policies</li> <li>• Reviewed and updated regularly</li> </ul>

<b>Controls</b>	<ul style="list-style-type: none"> <li>• The internal technology or tools the financial institution utilizes to ensure the AML/CFT program is functioning as intended and within predefined parameters.</li> <li>• Alerts compliance to potential outliers or deviations from normal policy that may need to be reviewed</li> <li>• Includes management reports, automated review systems or the utilization of multiple reviewers</li> </ul>
-----------------	---

## The Compliance Function

The compliance function is commonly referred to as the second line of defense. It is responsible for monitoring the controls of the business, also referred to as the first line of defense. As you read the following sections, it will become apparent that this function cannot be designed with a “one size fits all” mentality. Regardless of the structure, however, the role of the second line of defense must be established in a manner that ensures it can fulfill its role effectively.

The sophistication of the compliance function should be based upon the institution’s nature, size, complexity, regulatory environment and the specific risk associated with the products, services and clientele. No two institutions will have exactly the same compliance structure because the risk facing each institution is going to be different, as identified in their respective risk assessments.

## The Designation and Responsibilities of a Compliance Officer

In most cases, the board of directors is responsible for appointing a qualified individual as an institution’s AML/CFT Compliance Officer. This individual is responsible for managing all aspects of the AML/CFT compliance program. This includes, but is not limited to, designing and implementing the program, making necessary changes and updates, disseminating information about the program’s successes and failures to key staff members, constructing AML/CFT-related content for staff training programs and managing the institution’s adherence to applicable AML/CFT laws and regulations (including staying current on legal and regulatory developments in the field).

## COMMUNICATION

The ability of the compliance officer to communicate effectively, in both a written and verbal format, is vital to the success of an institution’s AML/CFT program. The compliance officer must also have the means to communicate at all levels of the organization—from front-line associates all the way up to the CEO and board of directors.

It is critical for a compliance officer to be capable of articulating matters of importance to senior and executive management, particularly significant changes that may present risk to the organization, such as a sudden or substantial increase in STRs or currency transaction reports (CTRs). Other items of concern that need to be escalated to management may include changes to laws or

regulations that may require immediate action. A compliance officer must have the skills necessary to be able to analyze and interpret these ongoing changes, determine what effect they may have on the institution and suggest an action plan when appropriate.

In many countries, the AML/CFT officer must also have a direct reporting line to the board or equivalent body. This unfettered access to board members allows him or her to undertake this oversight role in an effective manner. In other countries, different reporting lines may exist.

## DELEGATION OF AML DUTIES

The exact delegation of tasks and responsibilities in an AML/CFT department will vary among institutions. The department could potentially be organized into subgroups with, for example, one person responsible for strategic aspects of the program and another for its operational aspects, including suspected money laundering monitoring and reporting suspicious activity.

Examples of AML/CFT subgroups include the following.

- **Program Management**
  - Manages and coordinates regulatory examinations
  - Performs periodic reviews and updates of the program
  - Coordinates implementation activities with the lines of business and support groups to ensure that applicable business procedures get updated to incorporate program changes
  - Monitors regulatory environment for changes to the program
  - May be involved in preparing training materials and providing guidance and advice on more complicated AML/CFT issues not addressed by the line of business support group
- **Know Your Customer**
  - Assigns a risk code to all clients based on scoring of the CDD risk assessment
  - Performs additional due diligence on medium- and high-risk clients identified via the CDD process or clients seeking certain products/services from the financial institution
  - Provides a first line of contact for line-of-business questions on AML/CFT matters
- **Sanctions Screening**
  - Manages sanctions screening software applications or processes
  - Monitors and reconciles the data being received from the source systems
  - Fine-tunes the filter thresholds in accordance with changes in the risk profile of the organization
  - Reviews suspected matches and reports valid matches to the appropriate regulatory authorities
- **Transaction Monitoring**
  - Manages transaction-monitoring software applications

- Monitors and reconciles the data being received from the source systems
- Fine-tunes the filter thresholds in accordance with the changes in the risk profile of the organization
- Participates in the design of transaction-monitoring typologies and maintains the extensive documentation required
- **Financial Investigations**
  - Monitors alerts generated on customer transactions, such as those from automated systems and referrals from line of business staff.
  - Investigates such alerts and referrals and files STRs with the appropriate financial intelligence unit (FIU) as required

In addition to these groups, other AML/CFT tasks are often conducted in the business lines wherever there is customer contact. For example, CDD forms are often completed by account officers and others when a new account is opened while branch personnel participate in periodic reviews of high-risk clients and may be required to provide additional information or explanation to support investigations into potentially suspicious activity. Sometimes, suspicious activity may be reported to the Corporate Security group, which, upon determining that the activity might pose an AML/CFT risk, may refer the case to the Financial Investigations group.

The compliance department may also direct AML/CFT-related compliance efforts as a result of instructions from a regulatory authority or other research findings. The business and the compliance function may establish risk-based quality assurance reviews and monitoring and testing activities to ensure the functions are being performed appropriately. This may include a review of the CDD collected to ensure completeness, monitoring reports of CDD completeness or defects to ensure the systems are working as expected and performing tests to assess whether the monitoring and the business performance are satisfactorily measuring and ensuring compliance.

## COMPLIANCE OFFICER ACCOUNTABILITY

Regardless of the way an institution delegates its various AML/CFT tasks, the organization's designated compliance officer is responsible for the institution's overall AML compliance. More and more often various regulators are seeking enforcement actions against not only the institution, its executive management team and board of directors for AML/CFT violations, but the compliance officer as well.

### *Case Study*

In March 2016, FinCEN issued a civil money penalty against Thriftway Food Mart (an MSB), its owner and the institution's compliance officer for willful and repeated violations of the Bank Secrecy Act. The penalty was the result of an examination conducted in 2009 that revealed systematic AML, record keeping and reporting violations. The compliance officer admitted to improper conduct that resulted in a personal fine of \$10,000.

### *Case Study*

In December 2014, FinCEN imposed a \$1 million civil money penalty against MoneyGram's former Chief Compliance Officer (CCO) for failing to ensure that the company complied with AML and BSA laws. The CCO attempted to fight the penalties, but in January 2016 the United States District Court denied a motion to dismiss the complaint seeking to hold the CCO personally liable for the violations.

## AML/CFT Training

---

### COMPONENTS OF AN EFFECTIVE TRAINING PROGRAM

Most AML/CFT laws and regulations require financial institutions to have as part of their formalized AML/CFT compliance programs training for appropriate or relevant employees. Training is one of the most important ways to stress the importance of AML/CFT efforts, as well as educating employees about what to do if they encounter potential money laundering. Training also acts as an important control in the mitigation of money laundering risks to which the financial institution may be exposed.

An effective training program should not only explain the relevant AML/CFT laws and regulations, but also cover the institutions' policies and procedures used to mitigate money laundering risks. In this section, the term training will include both formal training courses and ongoing communications that serve to educate employees and maintain their ongoing awareness about AML/CFT requirements, such as emails, newsletters, periodic team meetings, intranet sites and other means that facilitate the sharing of information. Below is an outline of who should receive AML/CFT training, the topics that should form the basis of that training and how, when and where that training should be delivered.

### WHO TO TRAIN

The first step in designing an effective AML/CFT training program is to identify the target audience. Most areas of the financial institution should receive AML/CFT training. In some countries, training programs must extend beyond full- or part-time employees to include contractors, consultants, students or apprentice placements and secondees from other branches or subsidiaries. Each segment should be trained on AML/CFT topics and issues that are relevant to their activities.

#### *Example: Scope of Training*

- **Customer-facing staff:** This is the financial institution's first line of defense; the employees who need the deepest practical understanding of why AML/CFT efforts are important and what they need to do to be vigilant against money laundering. Although a general course will often be able to address the importance of AML and to provide some basics, some additional training on specific unit procedures related to the products and services carried out by the business line is often needed. For example, loans, credit and loan-operations staff need training on how money launderers might misuse credit products, how the staff might recognize potential money laundering and what the staff must do if they see it. Cash handlers often need special training because many jurisdictions have imposed additional requirements to

address the increased risk posed by cash. These employees need to know how to properly handle the cash transactions, especially those that trigger reporting requirements, including when to escalate concerns when a customer attempts to structure a transaction to avoid the reporting requirements. Employees establishing loans and accounts for new customers need to know applicable regulatory requirements and the institution's policies and procedures for identification and performing due diligence during the onboarding process.

- **Operations personnel:** Noncustomerfacing personnel within an organization's lines of business are also included in the first line of defense and should not be overlooked in the delivery of specialized training. For example, cash vault, wire transfer, trade finance, loan underwriters, loan collections and treasury management personnel are oftentimes in positions to recognize illegal, fraudulent or unusual account activity. Specialized training for these individuals to recognize AML/CFT red flags and elevate unusual activity to compliance personnel therefore should be considered.
- **AML/CFT compliance staff:** Under the direction of a designated compliance officer, this function coordinates and monitors the organization's day-to-day AML/CFT compliance program. It is the second line of defense. Given this area's responsibility for managing the organization's adherence to AML/CFT regulations, more advanced ongoing training to stay abreast of requirements and emerging trends is important. Often, this will require attending conferences or AML/CFT- specific presentations that are more robust in nature.
- **Independent testing staff:** Independent testing personnel are the organization's third line of defense. Because this functional area independently assesses the adequacy of the AML/CFT compliance program, these employees should receive periodic training concerning regulatory requirements, changes in regulation, money laundering methods and enforcement and their impact on the organization.
- **Senior management and board of directors:** The board and senior management do not need the same degree of training as personnel in the first, second or third lines of defense. Specialized training for the organization's leadership should address the importance of AML/CFT regulatory requirements, penalties for noncompliance, personal liability and the organization's unique risks. Without a general understanding of this information, senior management and the board cannot adequately provide for AML/CFT oversight, approve AML/CFT policies or provide sufficient resources.

## WHAT TO TRAIN ON

The next factor in designing an effective AML/CFT training program is identifying the topics to be taught. This will vary according to the institution and the specific products or services it offers.

Several basic matters should be factored into AML/CFT training.

- General background and history pertaining to money laundering controls, including the definitions of money laundering and terrorist financing, why criminals do it and why stopping them is important
- Legal framework on what AML/CFT laws apply to institutions and their employees

- Penalties for AML/CFT violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment
- Internal policies, such as customer identification and verification procedures and policies, including customer due diligence (CDD), enhanced due diligence (EDD) and ongoing due diligence
- Review of the internal AML/CFT and sanctions risk assessments
- Legal record-keeping requirements
- Suspicious transaction monitoring and reporting requirements
- Currency transaction reporting requirements
- How to react when faced with a suspicious client or transaction
- How to respond to customers who want to circumvent reporting requirements
- Duties and accountability of employees
- Maintaining confidentiality with AML-related matters
- AML trends and emerging issues related to criminal activity, terrorist financing and regulatory requirements
- Real-life money laundering schemes (preferably cases that have occurred at the institution or at similar institutions), including how the pattern of activity was first detected, its impact on the institution and its ultimate resolution

Parties responsible for designing the training must identify which of these topics relate to the target audience.

In April 2015, the United Kingdom's Financial Conduct Authority (FCA) published guidance to clarify expectations where significant AML weaknesses persist in small banks. The guidance was based on proposed examples of good practice from two thematic reviews that the FCA and its predecessor conducted. Among other issues, the FCA questioned the effectiveness of training programs, which often lacked specificity related to firms' unique risks. Training best practices published in the guidance included the following.

- Appropriate training tailored to the individual's specific roles. Roles lacking specific training included the following areas: offshore centers, mortgage lending, areas servicing PEPs and other high-risk clients, investment banks and trade finance. Generic training is considered to be acceptable provided it is supplemented with specific training with a practical application to the specific line of business or role within the organization.
- Periodic refresher training—usually annually—for existing employees
- Banks should assess whether third parties or employees working in outsourced functions need to attend specific AML training.

### Case Study

On February 25, 2016, FinCEN and the OCC coordinated enforcement actions against Gibraltar Private Bank and Trust Company, Coral Gables, Florida, for willful AML compliance violations. The bank's substantial AML program violations, which included failure to properly train compliance staff, led to a \$2.5 million civil money penalty assessed by the OCC and a \$4 million civil money penalty assessed by FinCEN. From 2009 to 2014, the bank's implementation of AML training was inadequate and not tailored to the needs of specific positions, departments, board members or other personnel. For example, in 2009, senior bank officials took a basic AML course specifically designed for tellers which was therefore not appropriate for their functional responsibilities. In May 2013, a training assessment was undertaken by management indicating a need for significant training necessary to adequately implement the bank's AML program. Over 1 year later, in 2014, regulatory authorities found that the bank had still not addressed any of the needs identified in its 2013 assessment.

## HOW TO TRAIN

Here are some steps that trainers can take to develop the how of an effective AML/CFT training program.

- Identify the issues that must be communicated and decide how best to disseminate the message. Sometimes a memo or email will accomplish what is needed without formal, in-person training. Sometimes, e-learning can efficiently do the job. Sometimes, classroom training is the best option.
- Identify the audience by functional area as well as by level of employee/management. This should be accompanied by a quick "Why are they here?" assessment. New hires should also receive training different from that given to veteran employees.
- Determine the needs that should be addressed. There may be issues uncovered by audits or regulatory examinations, or created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Determine if Train the Trainer sessions are necessary, where decentralized training is involved (e.g., across large branch networks).
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- To the extent possible, establish a training calendar that identifies the topics and frequency of each course.
- Consider whether to provide handouts. The purpose of most training handouts is either to reinforce the message of the training and to provide a reference tool after the fact.
- Tests should be considered as a means to evaluate how well the training is understood with a mandatory passing score and scores should be retained. Similarly, if a case study is used to illustrate a point, provide a detailed discussion of the preferred course of action.
- Attention span is a factor to consider. Focus on small, easy-to-digest, easy-to-categorize issues.

- Track attendance. Ask attendees to sign in, and issue reminders if make-up sessions are needed. Unexcused absences may warrant disciplinary action and notation in employee personnel files.

## **WHEN TO TRAIN**

An institution's training should be ongoing and on a regular schedule. Existing employees should at least attend an annual training session. New employees should receive appropriate training with respect to their job function and within a reasonable period after joining or transferring to a new job. Situations may arise that demand an immediate session. For example, an emergency training session may be necessary right after an examination or audit that uncovers serious money laundering control deficiencies. A news story that names the institution or recent regulatory action, such as a consent order, might also prompt quick-response training. Changes in software, systems, procedures or regulations are additional triggers for training sessions.

## **WHERE TO TRAIN**

Some institutions have training centers that allow trainees to escape the distractions of daily work activity. Some types of training are more effective when conducted in small groups, such as the evaluation of a money laundering case study. Role-playing exercises, which may be used to complement a prepared lecture or panel discussions are also more effective in small groups. These training sessions can be held anywhere. Large groups can be trained using computer-based training courses, which can be designed to automatically record attendance and test attendees (with a required minimum score to demonstrate understanding of the material).

# **Independent Audit**

---

## **EVALUATING AN AML/CFT PROGRAM**

Putting your AML/CFT compliance program into motion is not enough. The program must be monitored and evaluated. Institutions should assess their AML/CFT programs regularly to ensure their effectiveness and to look for new risk factors.

The audit must be independent (i.e., performed by people not involved with the organization's AML/CFT compliance staff), and individuals conducting the audit should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable. Depending on the jurisdiction, the independent audit may also be referred to as the independent test or independent review.

The independent audit should do the following.

- Assess the overall integrity and effectiveness of the AML/CFT compliance program, including policies, procedures and processes
- Assess the adequacy of the AML/CFT risk assessment

- Examine the adequacy of CDD policies, procedures and processes, and whether they comply with regulatory requirements
- Determine personnel adherence to the institution's AML/CFT policies, procedures and processes
- Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations)
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance
- Assess compliance with applicable laws and regulations based on the jurisdictions in which the organization does business
- Examine the integrity and accuracy of management information systems used in the AML/CFT compliance program. If applicable, this includes assessing the adequacy of the scope of any third-party independent system validations along with the qualifications of parties engaged to perform such reviews
- Review all the aspects of any AML/CFT compliance functions that have been outsourced to third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company
- Evaluate the ability of transaction monitoring software application to identify unusual activity by
  - reviewing policies, procedures and processes for suspicious activity monitoring;
  - reviewing the processes for ensuring the completeness, accuracy and timeliness of the data supplied by the source transaction processing systems;
  - evaluating the methodology for establishing and analyzing expected activity or filtering criteria;
  - evaluating the appropriateness of the monitoring reports; and
  - comparing the transaction monitoring typologies to the AML/CFT risk assessment for reasonableness.
- Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity
- Assess the effectiveness of the institution's policy for reviewing accounts that generate multiple suspicious transaction report filings, including account closure processes
- Assess the adequacy of record keeping and record retention processes
- Track previously identified deficiencies and ensure management corrects them promptly
- Decide whether the audit's overall coverage and frequency is appropriate to the risk profile of the organization

- In coordination with the board or designated board committee, ensure that overall audit coverage and frequency are appropriate to the risk profile of the organization
- Consider whether the board of directors was responsive to earlier audit findings
- Determine the adequacy of the following, as they relate to the training program and materials:
  - The importance the board and senior management place on ongoing education, training and compliance
  - Employee accountability for ensuring AML/CFT compliance, including the employee performance management process
  - Comprehensiveness of training, related to the risk assessment of each individual business line
  - Training of personnel from all applicable areas of the institution
  - Frequency of training including the timeliness of training given to new and transferred employees
  - Coverage of internal policies, procedures, processes and new rules and regulations
  - Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity
  - Disciplinary actions taken for noncompliance with internal policies and regulatory requirements

An effective internal audit department will develop and maintain an audit risk assessment to determine audit priorities. It will also develop and maintain detailed audit testing programs for every area.

All audit and regulatory recommendations for corrective action must track as well as indicate the target date for completion and the personnel responsible. Regular status reports should be provided to senior management and the board of directors. Supervisory authorities may request them. Failure to properly address audit issues is a frequent criticism in cases where regulators levy fines on institutions.

### Case Study

On June 15, 2015, FinCEN announced the assessment of a \$4.5 million civil money penalty (CMP) against Bank of Mingo in Williamson, West Virginia, for willfully violating the BSA. The bank entered into a \$2.2 million deferred prosecution agreement and forfeiture action with the U.S. Attorney's Office for the Southern District of West Virginia and was issued an order to pay a \$3.5 million CMP, announced by the Federal Deposit Insurance Corporation. Severe and systemic failures in many aspects of the bank's AML/CFT program were cited, including inadequate independent testing. The bank's independent testing failed to determine whether appropriate controls were in place to detect, monitor and report suspicious activity and large currency transactions. The scope of the most recent independent compliance testing, conducted in December 2011, failed to include high-risk activities, which led to more than \$9.2 million in structured and otherwise suspicious cash transactions flowing unreported through the institution from 2008 through 2012.

## Establishing a Culture of Compliance

---

Embedding a culture of compliance into the overall structure of a financial institution is critical to the development and ongoing administration of an effective AML/CFT program. Typically, the ultimate responsibility for the AML/CFT compliance program rests with the financial institution's board of directors. The board and senior management must set the tone from the top by openly voicing their commitment to the AML/CFT program, ensuring that their commitment flows through all service areas and lines of business and holding responsible parties accountable for compliance.

Although creating a culture of compliance may not resolve all current or future issues, an effective AML/CFT compliance program focused on identifying and controlling risks is critical to the overall success of an institution. There must be a clear understanding by associates in all business units of their commitment to playing by the rules. Adopting a culture of compliance is the most effective way to prevent easily identified issues from becoming systemic problems.

An adequate AML/CFT program costs money that management may be reluctant to spend. The compliance officer's challenge is to convince management that an AML/CFT program is an indispensable expense to protect the institution and to avert legal problems and reputational harm.

As a result of FinCEN's findings of numerous financial institutions with AML/CFT compliance deficiencies, including with the roles of boards and senior management, they released an advisory in August 2014. It suggested six guidelines for strengthening AML/CFT compliance culture in financial institutions.

1. Leadership must actively support and understand compliance efforts.

The board's role in AML/CFT compliance consists of reviewing and approving the overall AML/CFT program and ensuring that there is ongoing oversight. Board members are not expected to become AML/CFT experts nor are they responsible for day-to-day program management. Rather, they should be knowledgeable enough to formally approve an institution's AML/CFT compliance program and make sure it is adequately implemented and maintained by staff.

The board's oversight role also extends to the supervisor's examination process. Examiners routinely converse with the board and management before and during an on-site exam in order to gauge the board's commitment to compliance, its understanding of the law and its knowledge of how the institution operates. Once an exam by a supervisor or auditor is conducted, it is also the board's duty to ensure that any necessary corrective action is taken. Specific duties can be delegated but the board will be responsible if problems cited by the examiner or auditor are not corrected.

2. Efforts to manage and mitigate AML/CFT deficiencies and risk must not be compromised by revenue interests.

Compliance staff should be empowered with sufficient authority to implement an institution's AML/CFT policies. Revenue interests should not compromise or override compliance functions beyond the risk appetite of the institution. Essentially, compliance must not take a backseat to making money.

3. Relevant information from the various departments within the organization must be shared with compliance staff to further AML/CFT efforts.

Business units should not remain tethered within their own individual silos. Boundaries or barriers in communication should not exist within an institution. Relevant information should be shared with the AML/CFT compliance staff.

4. The institution must devote adequate resources to its compliance function.

In addition to the requirement of the designation of an individual responsible for coordinating and monitoring day-to-day AML/CFT compliance under the law, leadership should provide for technology resources as well as appropriate AML/CFT support staff based on its risk profile.

5. The compliance program must be effective. One way to ensure this is by using an independent and competent party to test the program.

To be effective, an AML/CFT program must include an ongoing documented risk assessment, risk-based customer due diligence and provide for testing by an independent, unbiased and qualified party.

6. Leadership and staff must understand the purpose of its AML/CFT efforts and how its STR reporting is used.

Leadership and AML/CFT staff should understand the importance of filing regulatory reports. Per FinCEN, properly filed reports are used “to confront serious threats, including terrorist organizations, rough nations, weapons of mass destruction (WMD) proliferators, foreign corruption and increasingly, some cyber-related threats.”

Further emphasizing the need for a culture of compliance, the New York State Department of Financial Services (DFS) issued Final Rule Part 504 on June 30, 2016, requiring regulated institutions to maintain Transaction Monitoring and Filtering Programs (TMPs) reasonably designed to

- monitor transactions after their execution for compliance with the BSA and AML laws and regulations, including suspicious activity reporting requirements; and
- prevent unlawful transactions with targets of economic sanctions administered by the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC).

The Final Rule, which went into effect on January 1, 2017, also requires boards of directors or senior officer(s) of regulated institutions to make annual certifications to the DFS confirming that they have taken all steps necessary to comply with the Transaction Monitoring and Filtering Program requirements.

Although the law may seem New York-specific, numerous foreign banks fall within the law because they operate in New York. Specifically, the law covers banks, trust companies, private bankers, savings banks and savings and loan associations chartered pursuant to the New York Banking Law and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York. Moreover, the law also applies to nonbank financial institutions (NBFIs) with a Banking Law license such as check cashers and money transmitters. Penalties for noncompliance consist of those under the Banking Law.

Importantly, the rule establishes eight minimum requirements for the Transaction Monitoring and Filtering Program, in addition to specific core components of each program that a financial institution must establish and maintain under the statute.

1. Identification of all data sources
2. Validation of the integrity, accuracy and quality of data
3. Data extraction and loading processes to ensure a complete and accurate transfer of data
4. Governance and management oversight
5. Vendor selection process if a third-party vendor is used
6. Funding to design, implement and maintain a program
7. Qualified personnel or outside consultant
8. Periodic training

The key to maximizing the AML/CFT unit's usefulness is to share valuable data with other areas of the firm, not just with law enforcement agencies, regulators and senior management. As AML/CFT units build their CDD files, they can identify information other departments can use to sell products and to expand profits. For example, marketing departments that better understand the activity of certain retail or business customers can more effectively identify opportunities to market additional products and deepen the overall customer relationship.

Before releasing customer information, it is important to review applicable privacy laws and the firm's privacy policy to understand any limitations. There are usually no regulatory problems with sharing customer information with other internal departments within the same legal entity; however, there may be limitations on sharing with other affiliated companies within a larger organization. Some firms restrict the sharing of customer information outside the organization and customers may opt-out of the right for the firm to provide their information to third-party companies.

Compliance staff should be sufficiently independent of the lines of business they support so that potential conflicts of interest are minimized; they should not be provided incentives based on the profitability of those business lines. This does not mean the compliance staff shouldn't receive bonuses; it means that incentives should not be structured in a way that might create a conflict of interest.

Although the compliance staff may sit within the line of business and report to line management, they should have the ability to escalate issues without fear of recrimination to a compliance or risk management function outside the line of business. This is not to say that the compliance staff should not be close to the line of business; on the contrary, a close working relationship with the line of business is crucial to a successful execution of the AML/CFT program. Ultimately, the compliance staff should be seen as trusted advisors so that the businessline staff will come to the compliance staff when they have questions and will follow the advice provided.

### *Case Study*

On May 24, 2016, the Monetary Authority of Singapore (MAS) announced that it ordered Switzerland's BSI Bank to shut down its operations as a merchant bank in Singapore for serious breaches of AML requirements, poor management oversight of the bank's operations and gross misconduct by some of the bank's staff. MAS has also served BSI Bank notice that it will impose financial penalties amounting to SG\$13.3 million for breaches of its Prevention of Money Laundering and Countering the Financing of Terrorism requirements. The breaches include failures to perform enhanced customer due diligence on high-risk accounts and to monitor for suspicious customer transactions on an ongoing basis.

Six members of BSI Bank's senior management and staff, including its chief executive, deputy chief executive and wealth management head were referred to the public prosecutor for possible criminal offenses.

## Know Your Customer

---

### CUSTOMER DUE DILIGENCE

A sound customer due diligence (CDD) program is one of the best ways to prevent money laundering and other financial crime. Knowledge is what the entire AML/CFT compliance program is built upon. The more the institution knows about its customers, the greater chance of preventing money laundering abuses. In fact, the U.S. Federal Financial Institutions Examination Council (FFIEC) in its November 2014 update to its BSA/AML Examination Manual said that the cornerstone of a strong AML compliance program is the adoption and implementation of comprehensive CDD policies, procedures and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. In most cases, normal and basic CDD collected will be sufficient. In other cases, further due diligence is required and may be extensive. The institution's CDD program must have a process in place to consider each level of due diligence that may be necessary.

In the FFIEC's view, the objective of CDD should be to enable the bank (or any financial institution) to predict with relative certainty the types of transactions in which the customer is likely to engage. These processes assist the financial institution in determining when transactions are potentially suspicious.

CDD is Recommendation 10 in FATF's updated Recommendations issued in February 2012. FATF recommends that financial institutions should be required to undertake CDD measures when

- establishing business relationships;
- carrying out occasional transactions under certain circumstances;
- there is a suspicion of money laundering or terrorist financing; and
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

## MAIN ELEMENTS OF A CUSTOMER DUE DILIGENCE PROGRAM

FATF recommends that institutions incorporate the following four measures into their CDD programs.

- Identifying the customer and verifying the customer's identity using reliable independent source documents, data or information
- Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business, risk profile and, where necessary, the source of funds.

A sound CDD program should include the seven elements outlined in the table below.

Element	Description
<b>Customer Identification</b>	Full identification of customer and business entities, including source of funds and wealth when appropriate. The institution should ensure there is a process in place to update and maintain current client information.
<b>Profiles</b>	Development of transaction and activity profiles for each customer. Profiles should contain sufficient information to allow for reviews of anticipated versus actual account activity or to otherwise enable the institution to identify suspicious activity based on comparing the activity to what it knows about the customer.
<b>Customer Acceptance</b>	Definition and acceptance of the customer in the context of their use of specific products and services, which may differ among clients and geographic markets.
<b>Risk rating</b>	Assessment and grading of risks presented by the customer's account relationship. Numerous factors should be considered when determining risk (e.g., client type, products and services, transactional activity and geographic locations). No single factor alone should be used to determine risk (except where such single factor constitutes an impermissible activity, such as violating economic sanctions or a business that is engaged in illegal activity).
<b>Monitoring</b>	Account and transaction monitoring based on the risks presented.
<b>Investigation</b>	Investigation and examination of unusual customer or account activity, which should be consistent with anticipated activity for each client based on his or her occupation or type of business.

Element	Description
<b>Documentation</b>	Documentation of findings as evidence or to provide a record of actions performed. “If it is not documented, it never happened.”

## ENHANCED DUE DILIGENCE

In its interpretive note to Recommendation 10, FATF acknowledges that there are circumstances where the risk of money laundering or terrorist financing is higher and enhanced CDD measures must be taken. Risk factors where enhanced CDD measures have to be taken include the following.

### Customer risk factors

- Unusual circumstances regarding how the business relationship is conducted, such as significant unexplained geographic distance between the financial institution and the customer
- Nonresident customers
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders or shares in bearer form
- Cash-intensive businesses
- Unusual or excessively complex appearance of the ownership structure of the company, given the nature of the company’s business

### Country or geographic risk factors

- Countries identified by credible sources, such as FATF’s mutual evaluations or detailed assessment reports, as not having adequate AML/CFT systems
- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations
- Countries identified by credible sources as having significant levels of drug trafficking, corruption, financial crimes or other criminal activity
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country
- Countries that share a common border and are known to have physical cross-border transactional activity
- Geographic areas identified as having a higher risk of money laundering or financial crimes, such as High Intensity Financial Crime Areas (HIFCA) and High Intensity Drug Trafficking Areas (HIDTA) in the United States

### Product, service, transaction or delivery channel risk factors

- Private banking
- Anonymous transactions (which may include cash)

- Nonface-to-face business relationships or transactions
- Payment received from unknown or unassociated third parties

The Basel Committee in its *Sound Management of Risks Related to Money Laundering and Terrorist Financing* states that EDD may be essential for an individual planning to maintain a large account balance and conduct regular cross-border wire transfers or an individual who is a politically exposed person.

## ENHANCED DUE DILIGENCE FOR HIGHER-RISK CUSTOMERS

Customers that pose higher money laundering or terrorist financing risks present increased exposure to financial institutions. Higher risk customers and their transactions should be reviewed even more closely at account opening and more frequently during their account relationships.

A financial institution should consider obtaining additional information from high-risk customers such as

- source of funds and wealth;
- identifying information on individuals with control over the account, such as signatories or guarantors;
- occupation or type of business;
- financial statements;
- banking references;
- domicile;
- proximity of the customer's residence, place of employment or place of business to the bank;
- description of the customer's primary trade area and whether international transactions are expected to be routine;
- description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and
- explanations for changes in account activity.

For higher risk customers, FATF also recommends obtaining the approval of senior management to commence or continue the business relationship and requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

## ACCOUNT OPENING, CUSTOMER IDENTIFICATION AND VERIFICATION

A sound CDD program should have reliable customer identification and account-opening procedures that allow the financial institution to determine the true identity of customers. Institutions should also set identification standards tailored to the risk posed by particular customers. In some countries, authorities have issued specific regulations and laws that set out what institutions are required to do regarding customer identification.

The Basel Committee in its January 2014 publication, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, states that a bank should establish a systematic procedure for identifying and verifying its customers and, where applicable, any person acting on their behalf and any beneficial owner(s). Although the committee focused on banks, its recommendations can apply to any financial institution that opens accounts.

A bank should not establish a banking relationship, or carry out any transactions, until the identity of the customer has been satisfactorily established and verified in accordance with FATF Recommendation 10. The identity of customers, beneficial owners and persons acting on their behalf, should be verified using reliable, independent source documents, data or information. Banks should be conscious that some identification documents are more vulnerable to fraud than others. For those that are most susceptible to fraud, or where there is uncertainty concerning the validity of the documents presented, the verification requirements should be enhanced and the information provided by the customer should be verified through additional inquiries or other sources of information.

Below are account opening and customer identification guidelines from Annex IV General Guide to Account Opening, issued in February 2016, as an attachment to the Basel Committee publication noted in the paragraph above. This document does not cover every eventuality; instead it focuses on some of the mechanisms banks can use in developing effective customer identification and verification programs.

The annex divides customers into two groups—natural people seeking to open an account and legal people and legal arrangements—and covers what types of information should be collected and verified for each.

Each new customer who is a natural person that opens a personal account should be asked for the following.

- Legal name (first and last) and any other names used (such as maiden name, former legal name or alias)
- Complete residential address and, on the basis of risk, also the business address or post office number
- Landline or mobile telephone numbers and email address
- Date and place of birth, and gender
- Nationality and residency status
- Occupation, position held and name of employer
- An official personal identification number or other unique identifier
- Type of account and nature of the banking relationship
- Signature

The institution should verify this information using reliable, independently sourced documents and data.

Documentary verification procedures include

- confirming the identity from an unexpired official document that bears a photograph of the customer;
- confirming the date and place of birth from an official document;
- confirming the validity of the official documentation through certification by an authorized person; and
- confirming the residential address

Nondocumentary verification procedures include

- contacting the customer by telephone or by letter to confirm the information supplied after an account has been opened;
- checking references provided by other financial institutions; and
- using an independent information verification process, such as by accessing public registers, private databases or other reliable independent sources.

In some jurisdictions, other documents of an equivalent nature may be offered as satisfactory evidence of a customer's identity.

Particular attention needs to be focused on those customers assessed as having higher risk profiles. Additional sources of information and enhanced verification procedures may include

- confirming an individual's residential address on the basis of official papers, a credit reference agency search or through home visits;
- prior bank reference (including banking group reference) and contact with the bank regarding the customer;
- verification of income sources, funds and wealth identified through appropriate measures;
- verification of employment and of public positions held; and
- personal reference from an existing customer of the financial institution.

If national law allows for nonface-to-face account opening, banks should take into account the specific risks associated with this method. Customer identification and verification procedures should be equally effective and similar to those implemented for face-to-face interviews. As part of broader CDD measures, the bank should consider, on a risk-sensitive basis, whether the information regarding sources of wealth and funds or destination of funds should be corroborated.

For legal people that are not natural people or legal arrangements, the following information should be obtained.

- Name, legal form status and proof of incorporation of the legal person
- Permanent address of the principal place of the legal person's activities
- Mailing and registered address of legal person

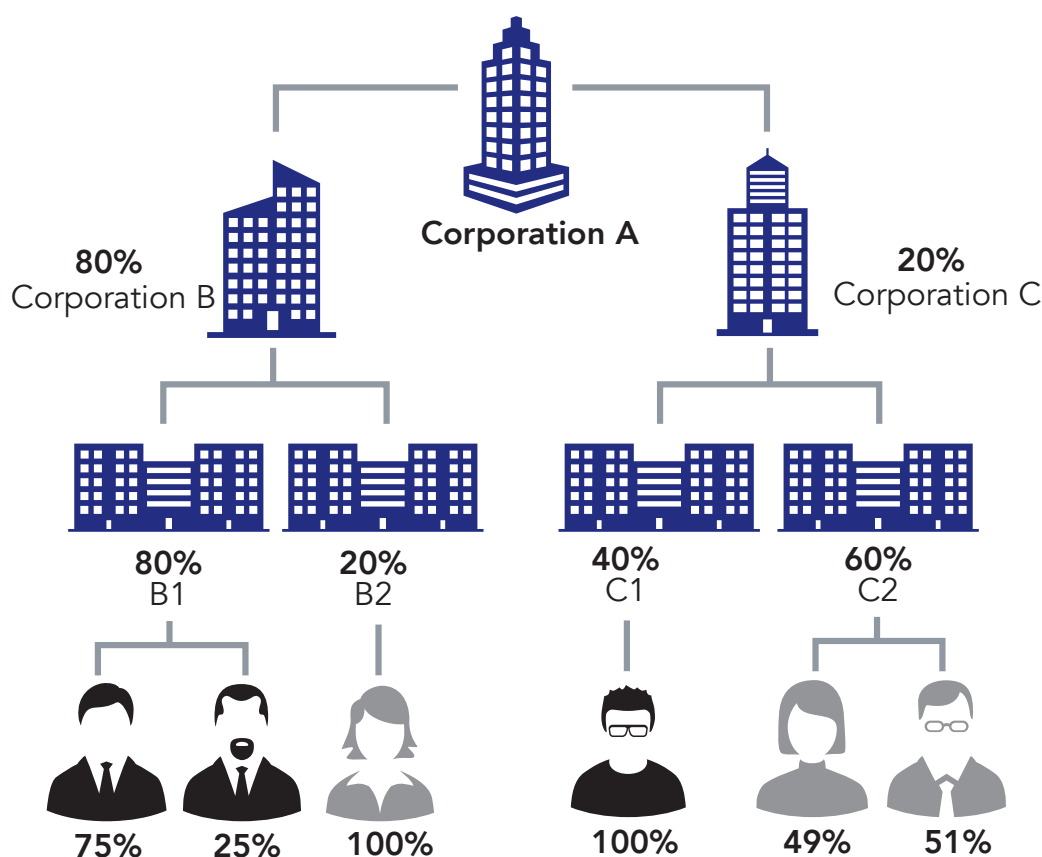
- Identity of natural people who are authorized to operate the account; in the absence of an authorized person, the identity of the relevant person who is the senior managing official
- Contact telephone numbers
- Official identification number
- Powers that regulate and bind the legal person
- Identity of the beneficial owners
- Nature and purpose of activities of the legal entity and its legitimacy
- Financial situation of the entity
- Expected use of the account—amount, number, type, purpose and frequency of the transactions expected—on the basis of risk; sources of funds paid into the account; and destination of funds passing through the account

The bank should verify the identity of the customer using reliable, independent source documents, data or information.

- Documentary verification methods include
  - obtaining a copy of the certificate of incorporation, memorandum and articles of association, partnership agreement or any other document certifying the existence of the entity; and
  - for established corporate entities, reviewing a copy of financial statements (audited, if available).
- Nondocumentary verification methods include
  - undertaking a company search and/or other commercial inquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved or terminated;
  - using an independent information verification process, such as by accessing public corporate registers, private databases or other reliable independent sources (e.g., lawyers, accountants);
  - validating the legal entity identifier and associated data in the public access service;
  - obtaining prior bank references;
  - visiting the corporate entity, where practical; and
  - contacting the corporate entity by telephone, mail or email.

The institution should verify that any person purporting to act on behalf of the legal person is so authorized. If so, banks should verify the identity of that person as well. Banks should also take reasonable steps to verify the identity of the beneficial owners. However, the exact account-opening procedures and customer acceptance policies will depend on the type of customer, the risk and the local regulations.

## Beneficial Ownership Structure Example



### Case Study

In 2011, FinCEN assessed a \$10.9 million civil money penalty against Ocean Bank (Ocean), the largest state chartered bank in Florida. FinCEN determined that Ocean violated the requirement to establish and implement an adequate AML program. For example, 28 percent of Ocean's total customers resided outside of the United States in high-risk geographies susceptible to money laundering, including Venezuela. Ocean established direct account relationships in the United States for politically exposed persons, consulates and established bearer share corporations. Given the high-risk nature of its account base, Ocean lacked adequate policies, procedures and an effective system of internal controls to assess and mitigate the risks of narcotics-related money laundering activity and to ensure the detection and reporting of suspicious transactions.

FinCEN found that

- Ocean did not adequately verify the identity and account-opening documents for foreign customer accounts—account-opening documents for Ocean's foreign customers arrived in the United States via mail pouch;
- Ocean opened accounts for customers in Venezuela without face-to-face contact;

- documentation of customer identification was not subject to adequate quality controls to ensure the accuracy of information;
- Ocean failed to maintain complete and sufficient documentation to develop appropriate customer profiles;
- Ocean's policies, procedures and controls failed to ensure that it gathered and reviewed sufficient information on foreign and domestic account customers to adequately assess risk and potential for money laundering; and
- a sampling of both foreign and domestic retail customer files showed errors and omissions in its documentation of specific customer information, including the nature of the customers' businesses, verification of owner/operator identities and anticipated account activity.

## CONSOLIDATED CUSTOMER DUE DILIGENCE

A fragmented CDD program can significantly increase the level of money laundering and terrorist financing risk a financial institution may face. One way to ensure financial institutions implement a strong CDD program is to consolidate and streamline account opening and ongoing monitoring processes across the organization, both domestically and globally where applicable.

Intergovernmental bodies have recognized the importance of implementing a consolidated CDD process and have provided specific guidance to financial institutions. According to the Basel Committee, a global risk management program for CDD should incorporate consistent identification and monitoring of customer accounts globally across business lines and geographical locations, as well as oversight at the parent level, in order to capture instances and patterns of unusual transactions that might otherwise go undetected. Such comprehensive treatment of customer information can significantly contribute to a bank's overall reputational, concentration, operational and legal risk management through the detection of potentially harmful activities, says the committee.

Financial institutions should aim to apply their customer acceptance policy, procedures for customer identification, process for monitoring higher risk accounts and risk management framework on a global basis to all of their offices, branches and subsidiaries. The firm should clearly communicate these policies and procedures through ongoing training and regular communications and conduct monitoring and testing to ensure compliance with the policies and procedures.

Each office, branch or subsidiary should be in a position to comply with minimum identification and accessibility standards applied by the parent. However, some differences in information collection and retention may be necessary across jurisdictions to conform to local regulatory requirements or relative risk factors such as areas that pose higher levels of risk related to money laundering, terrorist financing and corruption.

Where the minimum CDD standards of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two. Where this appears not to be possible, the institution should confer with its home office and attorneys to implement appropriate and effective CDD standards.

## Economic Sanctions

---

Economic sanctions are a way to financially isolate a target. Increasingly, countries are using economic sanctions instead of military force as an instrument of foreign policy. Sanctions can generally fall into one of the following categories.

- **Targeted sanctions:** aimed at specifically named individuals, such as key leaders in a country or territory, named terrorists, significant narcotics traffickers and proliferators of weapons of mass destruction. These sanctions often include the freezing of assets and travel bans where possible.
- **Sectoral sanctions:** aimed at key sectors of an economy to prohibit a very specific subset of financial dealings within those sectors to impede future growth.
- **Comprehensive sanctions:** generally prohibit all direct or indirect import/export, trade brokering, financing or facilitating against most goods, technology and services. These are often aimed at regimes responsible for gross human rights violations and nuclear proliferation.

Most jurisdictions impose sanctions regimes, particularly to comply with sanctions imposed by the United Nations and, for members, the European Union. As expected, with similar goals in their application, there is overlap in the sanctions applied by these bodies.

### UNITED NATIONS

U.N. Sanctions are managed by the U.N. Security Council Committees. The U.N. Security Council can take action to maintain or restore international peace and security under Chapter VII of the *United Nations Charter*. Sanctions measures, under Article 41, encompass a broad range of enforcement options that do not involve the use of armed force. Security Council sanctions have taken a number of different forms in pursuit of a variety of goals. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans and financial or commodity restrictions. The Security Council has applied sanctions to support peaceful transitions, deter nonconstitutional changes, constrain terrorism, protect human rights and promote nonproliferation.

### EUROPEAN UNION

Article 215 of the Treaty on the Functioning of the European Union (TFEU) provides a legal basis for the interruption or reduction, in part or completely, of the Union's economic and financial relations with one or more third countries (i.e., countries outside the EU), where such restrictive measures are necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP). In general terms, the EU imposes its restrictive measures to bring about a change in policy or activity by the target country, part of a country, government, entities or individuals. They are preventive, nonpunitive, instruments that allow the EU to respond swiftly to political challenges and developments. The EU has wielded measures in support of human rights and democracy objectives in the absence of a United Nations mandate and has supplemented U.N. sanctions to stop nuclear proliferation in Iran and North Korea.

## UNITED STATES

One of the best-known lists is the U.S. Treasury's Office of Foreign Assets Control's (OFAC) Specially Designated Nationals and Blocked Persons (SDN) list. Updated often, the SDN list contains thousands of names of individuals and businesses, as well as aircraft and ships (vessels) from more than 150 countries that the U.S. government considers to be terrorists, international narcotics traffickers or others covered by U.S. foreign policy and trade sanctions.

Under sanctions programs administered by OFAC, financial institutions are prohibited from providing property, or an interest in property, to a sanctions target (i.e., someone subject to a sanctions program). Depending on the particular program, this might mean blocking (or freezing) the transaction or it might mean rejecting (or returning) the transaction. The sanctions programs are governed by a number of laws and regulations and are subject to change; hence, sanctions compliance requires a specialized skillset and constant attention to the changing nature of sanctions.

OFAC is not a supervisory agency but works closely with supervisory agencies at both the federal and state levels. During examinations of financial institutions, supervisory examiners review OFAC compliance efforts, including policies and procedures, training, testing and tuning of screening systems, to determine a financial institution's ability to effectively detect SDNs and entities that are sanctioned within all of OFAC's programs—even entities that are not specially designated—and to comply with OFAC's sanction programs. If a financial institution is found to have weak OFAC controls or is engaged in activity with an entity identified on the SDN list or sanctioned under any OFAC sanction program, federal and state examiners and OFAC may take actions including, but not limited to, issuing monetary penalties, criminal penalties and regulatory actions (e.g., Written Agreements and Matters Requiring Attention).

## Sanctions List Screening

---

Before a financial institution starts doing business with a new customer or engaging in certain transactions (e.g., international wire payments), it should review the various country sanction program requirements as well as published lists of known or suspected terrorists, narcotics traffickers and other criminal actors for potential matches.

Institutions subject to sanctions compliance are required to screen customers and transaction records against periodically updated lists that include individuals and entities designated or identified by governmental bodies. Sanctions lists identify terrorists, terrorist organizations and supporters of terrorism, as well as those targeted by the three types of sanctions listed above.

Financial institutions must be alert to transactions that involve parties identified on a sanctions list. This is sometimes difficult, particularly because it relates to screening customer lists for people whose names are not originally in Roman characters, such as suspected terrorists from Middle Eastern countries or sanctions lists in Asian countries. For example, most of the names of designated terrorists on the OFAC SDN list also include numerous "also known as" alternatives. Although some names may be aliases, others are confusing because the customs are not understood. An understanding of Arab naming customs and protocols may help alleviate the confusion. Below are some helpful tips.

- All names are transliterated from an Arabic script in which short consonants are most often left out. So the name Mohammed might be written on a financial account as Mohamed or Mohamad.
- Arabic names are typically long. A person's second name is the father's name. If a bin or ibn precedes the name, it indicates "son of." If a family name is included at the end, it will sometimes have al preceding it.
- There is widespread use of certain names such as, Mohamed, Ahmed, Ali or any name with the prefix Abd- or Abdul, which means servant of, and is followed by one of 99 suffixes used to describe God.
- Many Arabic names begin with the word Abu. If it is a first name, it is probably not the person's given name, because Abu means father of. Abu, followed by a noun, means something like "freedom" or "struggle," and is used by both terrorists and legitimate political leaders. Only when Abu is a prefix of a surname should it be accepted as a given name.

## Politically Exposed Persons Screening

---

Although financial institutions take measures to develop robust procedures and screening processes to comply with sanctions or other customer screening requirements, these controls do not always detect suspicious high-risk individuals or businesses your organization needs to avoid and can sometimes fail. For example, intergovernmental bodies, such as FATF in its 40 Recommendations, make explicit reference to politically exposed persons (PEPs). And government regulations, specifically the Fourth European Union Anti-Money Laundering Directive, explicitly detail requirements related to PEPs; however, there still is no clear way to identify PEPs and their associates.

The problem is the lack of available and useful information about the identity of PEPs around the world. Currently, there are dozens of private providers that offer PEPs databases; however, the information contained in them, and the ability to positively match your customer with a PEP on a database, can be a challenge. In addition, as additional scrutiny continues to be placed on PEPs, they have gotten more creative in finding ways to avoid detection, such as opening accounts in the names of corporations (e.g., shell companies) in offshore jurisdictions instead of in their own names or the names of close family members. On the other hand, looking at geographical issues, the size and nature of an account and the purpose of the account may raise PEP-related issues.

There are some publicly available sources of information that can be used to assist you in identifying PEPs and their associates. The *Corruption Perceptions Index* published by Transparency International, an international, nongovernmental organization devoted to combating corruption, is useful in focusing on high-risk jurisdictions. Also, some government agencies, such as the U.S. Central Intelligence Agency, publish lists of heads of state and cabinet members of foreign governments. However, these lists do not provide all relevant information related to PEPs that would assist in identifying them. For instance, there is no unique identifier, such as a date of birth or address. This results in significant operational constraints, particularly at large retail financial institutions.

Accepting corruption proceeds from PEPs constitutes money laundering in the United States. Under some countries' laws it may be a violation of its sanctions rules. Yes, there is obvious difficulty in identifying these parties. That is why it is important to have strong customer due diligence and monitoring controls as these processes can assist in identifying PEPs.

It is also important to continually review and update customer screening and sanctions programs. This includes updating procedures, tuning and testing screening tools and training staff.

## **Know Your Employee**

---

Financial institutions and businesses have learned at great expense that an insider can pose the same money laundering threat as a customer. It has become clear in the AML/CFT field that having equivalent programs to know your customer and to know your employee are essential.

A Know Your Employee (KYE) program means that the institution has a program in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job descriptions, codes of conduct and ethics, levels of authority, compliance with personnel laws and regulations, accountability, monitoring, dual control and other deterrents should be firmly in place.

Background screening of prospective and current employees, especially for criminal history, is essential to keeping out unwanted employees and identifying those to be removed. The Federal Deposit Insurance Corporation (FDIC) has provided guidance on employee screening in its paper, *Pre-Employment Background Screening: Guidance on Developing an Effective Pre-Employment Background Screening Process*, issued in June 2005.

Background screening can be an effective risk-management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. Used effectively, the pre-employment background checks may: reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. An institution should also verify that contractors are subject to screening procedures similar to its own.

Costs are associated with developing and implementing an effective screening process. However, absent such a process, a bank may incur significant expenses in recruiting, hiring, training and ultimately terminating unqualified individuals.

Sometimes, regulations prohibit any person who has been convicted of a crime involving dishonesty or money laundering from becoming or continuing as an institution-affiliated party; owning or controlling, directly or indirectly, an institution; or otherwise participating, directly or indirectly, in the conduct of the affairs of an institution without the prior written consent of the regulator. Consultants who take part in the affairs of a financial institution may be subject to this requirement too.

Therefore, pre-employment background screening should be established by all financial institutions that, at a minimum, reveals information regarding a job applicant's criminal convictions. Sometimes, the level of screening should be raised. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification

of references, experience, education and professional qualifications, according to the FDIC. The Monetary Authority of Singapore's guidelines on employee hiring also includes screening against ML/TF information sources, bankruptcy searches and credit history checks.

Just as management verifies the identity of customers, it should also verify the identity of job applicants. Once the person is hired, an ongoing approach to screening should be considered for specific positions, as circumstances change or as needed for a comprehensive review of departmental staff over a period of time. Management should also have policies that address what to do when a screening uncovers information contrary to what the applicant or employee provided.

An institution may perform fingerprint checks periodically for employees in sensitive positions, or it may contract with a vendor to conduct an extensive background check when the employee is being considered for promotion to a high-level position. Without such screening procedures in place, financial institutions risk running afoul of the prohibition against employing statutorily disqualified individuals. The extent of the screening depends on the circumstances, with reasonableness being the standard.

In the UK, the Centre of Protection of National Infrastructure takes Know Your Employee a bit further and has made some very informative guidelines regarding insider threat and risk management. It includes examples of how insider threats or data leakages can have devastating effects on an organization. Within financial institutions this could include abuse of pre-market information only known by insiders. Many banks these days train their staff how to treat data in a transparent, customer-centric and law-abiding manner.

Regularly repeated training of employees regarding what is expected from them should be part of normal on-the-job training. With social media being an important day-to-day communication form for both private people and organizations, Know Your Employee programs might also require you to monitor what employees or insiders mention and like on their social media accounts. Social media accounts and posts on these accounts might give you ample information how a person might behave in an organization.

### Case Study

In October 2015, a banker pleaded guilty to a felony bank bribery charge in a San Diego, CA federal court that he caused Citibank to fail to report suspicious transactions and to maintain an effective AML/CFT compliance program. In his plea, the employee admitted that he used his position as well as his financial knowledge to aid his clients in avoiding detection by Citibank's AML/CFT compliance program. He did not report Citibank customers he knew were engaged in various suspicious and high-risk activities, undermined the bank's obligations in exchange for cash and in-kind compensation and counseled customers on the specifics of the bank's AML/CFT parameters by providing the customers with internal AML/CFT guidelines. Moreover, he devised schemes whereby shell bank accounts in nonthreatening business sectors were established and maintained by his clients for the purpose of engaging in large volumes of cash transactions without triggering the bank's AML/CFT reporting obligations. As of publication, he had not yet been sentenced.

## Suspicious or Unusual Transaction Monitoring and Reporting

---

Proper due diligence may require compliance personnel to gather further information regarding a customer or his or her transaction before deeming it suspicious and filing an STR. Although there are no hard and fast rules as to what constitutes suspicious activity, financial institution employees should watch for activity that may be inconsistent with a customer's source of income or regular business activities.

Because financial institutions must sort through thousands of transactions each day, a firm's system for monitoring and reporting suspicious activity should be risk-based and should be determined by factors such as the firm's size, the nature of its business, its location, the frequency and size of transactions and the types and geographical location of its customers.

Generally, the core operating system of a financial institution maintains significant customer data and can also be utilized to generate certain internal reports that can be used to discover possible money laundering and terrorist financing. Some of the reports can include

- daily cash activity in excess of the country's reporting threshold;
- daily cash activity just below the country's reporting threshold to identify possible structuring;
- cash activity aggregated over a period of time (e.g., individual transactions over a certain amount, or totaling more than a certain amount over a 30-day period) to identify possible structuring;
- wire transfer reports/logs with filters using amounts and geographical factors;
- monetary instrument logs/reports;
- check kiting/drawing on uncollected funds with significant debit/credit flows;
- significant change reports; and
- new account activity reports.

Although reporting procedures vary from country to country, a typical suspicious or unusual transaction reporting process within a financial institution as part of its AML/CFT program includes

- procedures to identify suspicious or unusual transactions or activity through various channels including employee observations or identification, inquiries from law enforcement or alerts generated by transaction monitoring systems;
- a formal evaluation of each instance, and continuation, of unusual transactions or activity;
- documentation of the suspicious transaction reporting decision (i.e., whether or not a report was filed with authorities);
- procedures to periodically notify senior management or the board of directors of suspicious transaction filings; and
- employee training on detecting suspicious transactions or activity.

Most countries that require suspicious transaction reporting prohibit disclosing the filing to the subject of the report (i.e., tipping off). In the United States, a financial institution and its directors, officers, employees and agents may not notify any person involved in the transaction that the transaction has been reported. Most laws also provide immunity from civil liability (safe harbor) to the filing institution and its employees.

The United States has even made it illegal to reveal information that would lead to knowledge of the existence of a suspicious activity report (SAR). This includes not only a prohibition on divulging the SAR itself, but also the fact that a SAR was or was not filed. For example, if a financial institution was asked whether it had filed a SAR, a failure to answer could indirectly indicate that a SAR had been filed. The confidentiality of SARs is a critical aspect of the whole reporting program as it protects financial institutions from being intimidated from filing reports. After all, the reports are meant to provide useful information to law enforcement and the threat of lawsuits by criminals should not deter financial institutions from fulfilling this important role.

Strong record-keeping procedures are key to managing any regulatory or legal implications of the filing. National laws or regulations usually dictate the length of time financial institutions and businesses must maintain records, the types of records that must be on hand and how they must be provided to regulatory or law enforcement personnel upon request.

There is no international clearinghouse for keeping STRs, but financial intelligence units in various countries often publish reports on how many STRs are filed each year, which areas are filing the most reports, what the suspicious activity or typology trends are and case studies. This information provides added guidance to financial institutions operating within their jurisdiction regarding their AML/CFT obligations.

---

## Automated AML/CFT Solutions

---

The sheer number of people and the volume of regulations and data involved in complying with regulations make manual AML/CFT compliance difficult, if not impossible. Most institutions have designated technology systems to automate their compliance activities, whereas a few still undertake their efforts manually.

Appropriately functioning technology can equip financial institutions with improved defenses in the fight against financial crime by providing the following.

- **Automated customer verification:** Using third-party databases to compare information provided by a customer with source data.
- **Watch list filtering:** Screening new accounts, existing customers, beneficiaries and transaction counterparties against terrorist, criminal and other blocked-persons sanctions and/or watch lists.
- **Transaction monitoring:** Scanning and analyzing transactional data for potential money laundering activity.
- **Automation of regulatory reporting:** Filing suspicious transaction reports (STRs), currency transaction reports (CTRs) or other regulatory reports with the government.

- **Case management:** Providing a dashboard feature to view customer KYC, transaction history and any investigations undertaken or regulatory filings filed on a customer.
- **Audit trail:** Documenting steps taken to demonstrate compliance efforts to auditors and supervisory authorities.

Automation is used for more than increased efficiency and control. It also may reflect a company's commitment to meet or exceed compliance requirements. A byproduct of this commitment is that regulators can receive prompt, concise and formatted information.

Many software companies offer technology dedicated to combat laundering, whereas some organizations have internally generated electronic systems. Before designing an AML/CFT compliance program or purchasing new technology, the financial institution should review the feasibility, costs and benefits to be derived from each course of action.

Some financial institutions choose to take the plunge and opt for AML/CFT software packages. Many will use a Request For Proposal (RFP) method. The institution will send out RFPs to software providers that it believes may be qualified to participate. An RFP lists project specifications and application procedures. The objective of the RFP is to select a system that may assist the institution in completing its responsibilities under applicable money laundering regulations. The system(s) may help identify potentially high-risk customers, accounts and transactions and may aid in conducting, managing and documenting any resulting investigations, as well as streamlining the completion and filing of any required STRs.

Most institutions seek a partner with a longstanding commitment to stay ahead of the rapidly changing regulatory landscape and with a track record that reflects flexibility, agility and urgency in delivering features that improve clients' efficiency in monitoring the right transactions and investigating the right clients. Ideally, the system is flexible, fast and efficient to deploy. It should allow the institution to navigate seamlessly around client relationships, accounts and transactions across a variety of product lines and systems, including deposits, wires, transfers, loans, trust, brokerage, letters of credit and check-imaging applications. A single view into clients' relationships is of paramount importance in delivering efficient, reliable and instant access to information. Each institution will have to identify the vendor that best meets its needs. During the RFP process, most institutions form evaluation teams composed of management from compliance, operations, technology and business departments. The team, facilitated by the project manager, will be responsible for reviewing and scoring all responses to the RFP.

Determining the most applicable system for a financial institution depends on its customer base, size and services offered. In general, a financial institution should consider the following capabilities of the system during its assessment process.

- Ability to monitor transactions and identify anomalies that might indicate suspicious activity
- Ability to gather CDD information for new and existing customers, score customer responses and store CDD data for subsequent use
- Ability to conduct advanced evaluation and analysis of suspicious/unusual transactions identified by the monitoring system in the context of each client's risk profile and that of his or her peer group

- Ability to view individual alerts within the broader context of the client's total activity at the institution
- Workflow features, including the ability to create a case from an alert or series of alerts, to collaborate (simultaneous or serial) among multiple interested parties to view and update information and to share AML/CFT-related information across monitoring and investigating units and throughout the bank as needed
- Ability to use data from the institution's core customer and transaction systems and databases to inform/update monitoring and case management activities
- Ability to store and recall at least 12 months' data for trend analysis
- Ability to manage the assignment, routing, approval and ongoing monitoring of suspicious activity investigations
- Automated preparation and filing of STRs to the financial intelligence unit
- Standard and ad-hoc reporting on the nature and volume of suspicious activity investigations and investigator productivity for management and other audiences
- Enhanced ability to plan, assign and monitor the caseload per employee of AML-related investigations
- Ability to provide comprehensive and accurate reporting of all aspects of AML compliance, including reporting to management, reporting to regulators, productivity reporting and ad-hoc reporting
- User-friendly updating of risk-parameter settings without the need for special technical computing skills
- Tiered user-rights access for users, managers and auditors

In addition to the above features, financial institutions should evaluate the following aspects of an automated system.

- Ease of use of the application, as well as the configuration of new and changed transaction monitoring rules
- Ease of data integration, system implementation and configuration
- Scalability of application; the ability of the system to grow with the institution
- Extent to which the system can be supported with internal resources
- User satisfaction with hardware and software support
- Price, including initial cost, ongoing costs to sustain the system or to expand the capabilities of the system, both in terms of what the vendor will charge and how much the institution will need to spend in terms of dollars, personnel and technology capacity

In addition to providing possible regulatory compliance solutions, automated tools may help an institution analyze how customers and users are using its products and services. For marketing purposes, patterns of activity among types of clients and different business lines can be represented by graphs and statistical reports. Depending on an institution's needs, a variety of software products can automate these tasks—from standard analytical systems to sophisticated artificial intelligence.

Automated tools may also help with documentation management, which can be a large burden for many financial institutions. Historically, imaging systems offered quick and paperless access to records. Convenience is not enough anymore, and technology has gone one step further. New systems can track and report the status of all documents, including those that are missing or expired. One-stop access systems can provide images as well as standardization and control for documents that must be accounted for and produced for compliance purposes.

## **Money Laundering and Terrorist Financing Red Flags**

---

Although there is no exhaustive list of tried-and-true suspicious activity indicators for businesses, there are many common indicators of financial crime, money laundering and terrorist-financing activity that your institution can be ready for.

Methods of money laundering have become more sophisticated as the complexity of financial relationships has grown, and paths through which funds move worldwide through financial institutions have multiplied. There is also a concern over worldwide terrorist threats. Financial institutions and NBFIs play a critical part in efforts to disrupt movement of funds used to support and carry out terrorist attacks. Although it may be difficult to detect terrorist financing transactions, there is guidance available from a variety of authoritative sources. Red flag indicator guidance should be used when building out or refining transaction monitoring programs.

The following situations may warrant additional scrutiny as they can indicate money laundering or terrorist financing. These lists are not exhaustive but should help to determine whether the activity is suspicious or does not appear to have a reasonable business or legal purpose.

### **UNUSUAL CUSTOMER BEHAVIOR**

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses a financial institution's record-keeping or reporting requirements with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record keeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be reported.
- Customer suggests paying a gratuity to an employee.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.
- Customer, who is a public official, opens account in the name of a family member who begins making large deposits not consistent with the known sources of legitimate family income.

- Customer, who is a student, uncharacteristically transfers or exchanges large sums of money.
- Account shows high velocity in the movement of funds, but maintains low beginning and ending daily balances.
- Transaction involves offshore institutions whose names resemble those of well-known legitimate financial institutions.
- Transaction involves unfamiliar countries or islands that are hard to find on an atlas or map.
- Agent, attorney or financial advisor acts for another person without proper documentation, such as a power of attorney.

### **UNUSUAL CUSTOMER IDENTIFICATION CIRCUMSTANCES**

- Customer furnishes unusual or suspicious identification documents or declines to produce originals for verification.
- Customer is unwilling to provide personal background information when opening an account.
- Customer tries to open an account without identification, references or complete local address.
- Customer's permanent address is outside of the institution's service area.
- Customer's home or business telephone is disconnected.
- Customer does not wish a statement of his or her account or any mail sent to him or her.
- Customer asks many questions about how the financial institution disseminates information about the identification of its customers.
- A business customer is reluctant to provide complete information about the nature and purpose of its business, anticipated account activity and other details about the business or to provide financial statements or documents about a related business entity.
- Customer provides no record of past or present employment on a loan application.
- Customer's Internet Protocol (IP) address does not match the identifying information provided during online registration.

### **UNUSUAL CASH TRANSACTIONS**

- Customer makes large cash deposit without having counted the cash.
- Customer frequently exchanges small bills for large bills.
- Customer's cash deposits often contain counterfeit bills or musty or extremely dirty bills.
- Customer comes in with another customer and they go to different tellers to conduct currency transactions under the reporting threshold.
- Customer makes large cash deposit containing many larger denomination bills.

- Customer opens several accounts in one or more names, and then makes several cash deposits under the reporting threshold.
- Customer withdraws cash in amounts under the reporting threshold.
- Customer withdraws cash from one of his or her accounts and deposits the cash into another account the customer owns.
- Customer conducts unusual cash transactions through night deposit boxes, especially large sums that are not consistent with the customer's business.
- Customer makes frequent deposits or withdrawals of large amounts of currency for no apparent business reason or for a business that generally does not generate large amounts of cash.
- Customer conducts large cash transactions at different branches on the same day, or coordinates others to do so on his or her behalf.
- Customer deposits cash into several accounts in amounts below the reporting threshold and then consolidates the funds into one account and wire transfers them abroad.
- Customer attempts to take back a portion of a cash deposit that exceeds the reporting threshold after learning that a currency transaction report will be filed.
- Customer conducts several cash deposits below the reporting threshold at ATMs.
- Corporate account has deposits or withdrawals primarily in cash, rather than checks.
- Customer frequently deposits large sums of cash wrapped in currency straps.
- Customer makes frequent purchases of monetary instruments with cash in amounts less than the reporting threshold.
- Customer conducts an unusual number of foreign currency exchange transactions.
- Customer indulges in foreign exchange transactions/currency swaps without caring about the margins.
- Noncustomer deposits cash into a customer account, which was subsequently withdrawn in a different geographic location

## UNUSUAL NONCASH DEPOSITS

- Customer deposits a large number of traveler's checks, often in the same denominations and in sequence.
- Customer deposits large numbers of consecutively numbered money orders.
- Customer deposits checks and/or money orders that are not consistent with the stated purpose of the account or nature of business.
- Customer deposits a large number of third-party checks.
- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

## UNUSUAL WIRE TRANSFER TRANSACTIONS

- Wire transfers are sent or received from the same person to or from different accounts.
- Nonaccount holder sends wire transfer with funds that include numerous monetary instruments, each in an amount under the reporting threshold.
- An incoming wire transfer has instructions to convert the funds to cashier's checks and to mail them to a nonaccount holder.
- Wire transfer activity to and from secrecy havens or higher risk geographic locations without apparent business reason or is inconsistent with a customer's transaction history.
- An incoming wire transfer, followed by an immediate purchase by the beneficiary of monetary instruments for payment to another party.
- An increase in international wire transfer activity in an account with no history of such activity or where the stated business of the customer does not warrant it.
- Customer frequently shifts purported international profits by wire transfer out of the country.
- Customer receives many small incoming wire transfers and then orders a large outgoing wire transfer to another country.
- Customer deposits bearer instruments followed by instructions to wire the funds to a third party.
- Account in the name of a currency exchange house receives wire transfers and/or cash deposits under the reporting threshold.

## UNUSUAL SAFE DEPOSIT BOX ACTIVITY

- Customer spends an unusual amount of time in the safe deposit box area, possibly indicating the safekeeping of large amounts of cash.
- Customer often visits the safe deposit box area immediately before making cash deposits of sums under the reporting threshold.
- Customer rents multiple safe deposit boxes.

## UNUSUAL ACTIVITY IN CREDIT TRANSACTIONS

- A customer's financial statement makes representations that do not conform to accounting principles.
- A transaction is made to appear more complicated than it needs to be by use of impressive but nonsensical terms such as emission rate, prime bank notes, standby commitment, arbitrage or hedge contracts.
- Customer requests loans either made to offshore companies or secured by obligations of offshore banks.
- Customer suddenly pays off a large problem loan with no plausible explanation as to the source of funds.

- Customer purchases certificates of deposit and uses them as collateral for a loan.
- Customer collateralizes a loan with cash deposits.
- Customer uses cash collateral located offshore to obtain a loan.
- Customer's loan proceeds are unexpectedly transferred offshore.

### **UNUSUAL COMMERCIAL ACCOUNT ACTIVITY**

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.
- Retail business that provides check-cashing services does not make withdrawals of cash against check deposits, possibly indicating that it has another source of cash.
- Customer maintains an inordinately large number of accounts for the type of business purportedly being conducted.
- Corporate account shows little or no regular, periodic activity.
- A transaction includes circumstances that would cause a banker to reject a loan application because of doubts about the collateral.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- Transacting businesses share the same address, provide only a registered agent's address or raise other address-related inconsistencies.

### **UNUSUAL TRADE FINANCING TRANSACTIONS**

- Customer seeks trade financing on the export or import of commodities whose stated prices are substantially more or less than those in a similar market situation or environment.
- Customer requests payment of proceeds to an unrelated third party.
- Significantly amended letters of credit without reasonable justification or changes to location of payment or the beneficiary just before payment is made.
- Customer changes the place of payment in a letter of credit to an account in a country other than the beneficiary's stated location.
- Customer's standby letter of credit is used as a bid or performance bond without the normal reference to an underlying project or contract, or designates unusual beneficiaries.
- Letter of credit is inconsistent with customer's business.
- Letter of credit covers goods that have little demand in importer's country.
- Letter of credit covers goods that are rarely if ever produced in the exporter's country.

- Documents arrive without title documents.
- Letter of credit is received from countries with a high risk for money laundering.
- Obvious over- or underpricing of goods and services.
- Transaction's structure appears unnecessarily complex and deigned to obscure the true nature of the transaction.
- Commodities are shipped through one or more jurisdictions for no apparent economic or logistical reason.
- Transaction involves the use of repeatedly amended or frequently extended letters of credit.
- Size of the shipment appears inconsistent with the regular volume of business of the importer or of the exporter.

### **UNUSUAL INVESTMENT ACTIVITY**

- Customer uses an investment account as a pass-through vehicle to wire funds to offshore locations.
- Investor seems uninterested in the usual decisions to be made about investment accounts, such as risks, commissions, fees or the suitability of the investment vehicles.
- Customer wants to liquidate a large position through a series of small transactions.
- Customer deposits cash, money orders, traveler's checks or cashier's checks in amounts under the reporting threshold to fund an investment account.
- Customer cashes out annuities during the free look period or surrenders the annuities early.

### **OTHER UNUSUAL CUSTOMER ACTIVITY**

- Customer conducts an unusually high level of transactions over the Internet or by telephone.
- Customer purchases a number of open-end prepaid cards for large amounts, inconsistent with normal business activity.
- Funds withdrawn from the accounts are not consistent with the normal business or personal activity of the account holder or include transfers to suspicious international jurisdictions.
- Customer uses a personal account for business purposes.
- Customer repeatedly uses bank or branch locations geographically distant from customer's home or office without sufficient business purpose.

### **UNUSUAL EMPLOYEE ACTIVITY**

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires.
- Employee is involved in an excessive number of unresolved exceptions.

- Employee lives a lavish lifestyle that could not be supported by his or her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.
- Employee uses company resources to further private interests.
- Employee assists transactions where the identity of the ultimate beneficiary or counter party is undisclosed.
- Employee avoids taking periodic vacations.

### **UNUSUAL ACTIVITY IN A MONEY REMITTER/ CURRENCY EXCHANGE HOUSE SETTING**

- Unusual use of money orders, traveler's checks or funds transfers.
- Two or more people working together in transactions.
- Transaction altered to avoid filing a CTR.
- Customer comes in frequently to purchase less than \$3,000 in instruments each time (or whatever the local record-keeping threshold is).
- Transaction altered to avoid completion of record of funds transfer, money order or traveler's checks of \$3,000 or more (or whatever the local record-keeping threshold is).
- Same person uses multiple locations in a short time period.
- Two or more people use the same identification.
- One person uses multiple identification documents.

### **UNUSUAL ACTIVITY FOR VIRTUAL CURRENCY**

- Repeated receipt of funds transfers from VC exchanges inconsistent with customer profile.
- Multiple transfers going to one common end user.
- Transactions involving virtual currency exchanges are followed within a short time by funds transfers to or ATM withdrawals in high-risk geographies.
- Purchase of VC shortly following receipt of funds transfers from unconnected third parties.
- Multiple accounts are used to collect and funnel funds to a small number of VC accounts.
- Multiple purchases of virtual currency at or just below \$3,000 record-keeping requirement.
- Key words entered into the transaction that could relate to the sale of suspicious products.

### **UNUSUAL ACTIVITY IN AN INSURANCE COMPANY SETTING**

- Cash payments on insurance policies.

- Use of multiple currency equivalents (e.g., cashier's checks and money orders) different sources to make insurance policy or annuity payments.
- Purchases of products that appear outside the customer's normal range of financial wealth or estate planning needs.
- Refunds requested during a policy's legal cancellation period or free-look period.
- Policy premiums paid from abroad, especially from an offshore financial center.
- A policy calling for the periodic payment of premiums in large amounts.
- Changing the named beneficiary of a policy to a person with no clear relationship to the policyholder.
- Lack of concern for significant tax or other penalties assessed when canceling a policy.
- Redemption of insurance bonds originally subscribed to by an individual in one country by a business entity in another country.

## UNUSUAL ACTIVITY IN A BROKER-DEALER SETTING

In 2002, the U.S. National Association of Securities Dealers (NASD), a self-regulatory organization that oversees the NASDAQ Stock Market under the authority of the U.S. Securities and Exchange Commission, offered in its Special NASD Notice to Members signs of suspicious activity to the securities field.

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information, or is otherwise evasive regarding that person or entity.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of interaccount or third-party transfers.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds from the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner so as to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S (Reg S) stocks and bearer bonds, which, although legitimate, have been used in connection with fraudulent schemes and money laundering activity.

- The customer's account shows an unexplained high level of activity with very low levels of securities transactions.

## UNUSUAL REAL ESTATE ACTIVITY

- Borrower/buyer submits invalid documents in order to cancel mortgage obligations or to pay off his or her loan balances(s).
- Same notary public and/or other authorized representative working with and/or receiving payments from an unusually large number of borrowers.
- Falsification of certified checks, cashier's checks or noncash item checks drawn against a borrower/buyer's account, rather than from the account of a financial institution.
- Borrower/buyer applies for a loan for a primary residence but does not reside in the new primary residence as indicated on the loan application; other individuals occupy the borrower/buyer's new primary residence indicating the property is being used as a secondary residence or income-generating property.
- Borrower/buyer requests refinancing for primary residence when public and personal documents indicate that the borrower/buyer resides somewhere other than the address on the loan application.
- Low appraisal values, nonarms length relationships between short sale buyers and sellers, or previous fraudulent sale attempts in short-sale transactions.
- Agent of the buyer and/or seller in mortgage transaction is unlicensed.
- Past misrepresentations made by borrower/buyer in attempts to secure funding, property, refinance and/or short sales.
- Improper/incomplete file documentation, including borrower/buyer reluctance to provide more information and/or unfulfilled promises to provide more information.
- Apparent resubmission of rejected loan application with key borrower/buyer details changed or modified from individual borrower to company/corporation; this activity may identify the same person attempting to secure a loan fraudulently through a straw-borrower or nonexistent person.
- Borrower/buyer attempts to structure currency deposits/withdrawals, or otherwise to hide or disguise the true value of assets, in order to qualify for loan modification programs intended for those homeowners in financial distress.
- Request from third-party affiliates on behalf of distressed homeowners to pay fees in advance of the homeowner receiving mortgage counseling, foreclosure avoidance, a loan modification or other related service.
- Third-party solicitation of distressed homeowners for purported mortgage counseling, foreclosure avoidance, loan modification or other related services; these third parties may also claim to be associated with legitimate mortgage lenders, the U.S. government or a U.S. government program.

## UNUSUAL ACTIVITY FOR DEALERS OF PRECIOUS METALS AND HIGH-VALUE ITEMS

The October 2013 FATF Report, *Money Laundering and Terrorist Financing Through Trade in Diamonds*, describes transactional and other red-flag indicators related to trade practices. They are listed below.

- Diamonds originate from a country where there is limited production or no diamond mines at all.
- Trade in large volumes conducted with countries that are not part of the diamond pipeline.
- Volume of purchases and/or imports that grossly exceed the expected sales amount.
- Sale of gold bars, coins and loose diamonds from a jewelry store (retail).
- An increase of the volume of the activity in a diamond dealer's account despite a significant decrease in the industry-wide volume.
- Selling and buying diamonds between two local companies through an intermediary located abroad (lack of business justification and/or uncertainty as to actual passage of goods between companies).
- Payments related to the appearance of rare or unique diamonds in the international market outside of known trading procedures (e.g., Argyle's rare pink diamond appearing in the international marketplace outside of the annual tender process).
- A single bank account is used by multiple businesses.
- A single bank account has multiple deposit handlers (retail and wholesale).
- Use of third parties to deposit funds into a single or multiple diamond dealers' accounts.
- Financial activity is inconsistent with practices in the diamond trade.
- Deposits or transfers to a diamond dealer's account from foreign companies followed by immediate transfer of similar amounts to another jurisdiction.
- Open export is settled by offsetting to, and receiving payment from, a third party.
- Receiving/transferring funds for import/export where the ordering customer/beneficiary is an MSB.
- Name of receiver in the payment from the diamond dealer is not the exporter/supplier.

## UNUSUAL ACTIVITY INDICATIVE OF TRADE-BASED MONEY LAUNDERING

- Payment made via virtually any method (cash, wire, check, bank drafts, etc.) by a third party with no connection to the underlying transaction.
- Structured currency deposits to individual checking accounts with multiple daily deposits to multiple accounts at different branches of the same bank on the same day.

- Discrepancies in the description of goods or commodity in the invoice or of the actual goods shipped.
- Amended letters of credit without justification.
- No apparent business relationship between the parties and transactions.
- Frequent transactions in round or whole dollars.
- Funds transferred into an account and moved to a high-risk country in the same amount.
- Companies operating in jurisdictions where their business purpose is not fully understood and there are difficulties in determining ownership.
- Lack of appropriate documentation to support transactions.
- Negotiable instruments used to fund transactions in sequential numbers and/or missing payee information.

## UNUSUAL ACTIVITY INDICATIVE OF HUMAN SMUGGLING

According to FinCEN's 2014 Advisory, *Guidance on Recognizing Activity That May Be Associated With Human Smuggling and Human Trafficking—Financial Red Flags*, the following are red flags for human smuggling.

- Multiple wire transfers, generally kept below the \$3,000 reporting threshold, sent from various locations across the United States to a common beneficiary located in a U.S. or Mexican city along the southwest border.
- Multiple wire transfers conducted at different branches of a financial institution to or from U.S. or Mexican cities along the southwest border on the same day or on consecutive days.
- Money flows that do not fit common remittance patterns.
  - Wire transfers that originate from countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) are directed to beneficiaries located in a U.S. or Mexican city along the southwest border.
  - Beneficiaries receiving wire transfers from countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) who are not nationals of those countries.
- Unusual currency deposits into U.S. financial institutions, followed by wire transfers to countries with high migrant populations (e.g., Mexico, Guatemala, El Salvador, Honduras) in a manner that is inconsistent with expected customer activity. This may include sudden increases in cash deposits, rapid turnover of funds and large volumes of cash deposits with unknown sources of funds.
- Multiple, apparently unrelated, customers sending wire transfers to the same beneficiary, who may be located in a U.S. or Mexican city along the southwest border. These wire senders may also use similar transactional information including but not limited to common amounts, addresses and phone numbers. When questioned to the extent circumstances allow, the wire senders may have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.

- A customer's account appears to function as a funnel account, whereby cash deposits (often kept below the \$10,000 reporting threshold) occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.
- Checks deposited from a possible funnel account appear to be pre-signed, bearing different handwriting in the signature and payee fields.
- Frequent exchange of small denomination for larger denomination bills by a customer who is not in a cash-intensive industry. This type of activity may occur as smugglers ready proceeds for bulk cash shipments.
- When customer accounts near the southwest border are closed due to suspicious activity, new customers may begin transacting on behalf of those customers whose accounts have been closed; this may be done as a means to continue illicit activities. In this case, new accounts often reflect activity similar to that of the closed accounts where transactions may be frequently occurring, currency-intensive and involve individuals that used to receive/send funds from/to accounts previously closed due to suspicious activity.
- Unexplained/unjustified lifestyle incommensurate with employment or business line; profits/deposits significantly greater than that of peers in similar professions/business lines.
- Inflows are largely received in cash where substantial cash receipts are inconsistent with the customer's line of business; extensive use of cash to purchase assets and to conduct transactions.

## UNUSUAL ACTIVITY INDICATIVE OF HUMAN TRAFFICKING

According to FinCEN's 2014 Advisory, *Guidance on Recognizing Activity That May Be Associated With Human Smuggling and Human Trafficking—Financial Red Flags*, the following are red flags for human trafficking.

- A business customer does not exhibit normal payroll expenditures (e.g., wages, payroll taxes, social security contributions); payroll costs can be nonexistent or extremely low for the size of the customer's alleged operations, workforce and/or business line/model.
- Substantial deductions to wages. To the extent a financial institution is able to observe, a customer with a business may deduct large amounts from the wages of its employees alleging extensive charges (e.g., housing and food costs), where the employees only receive a small fraction of their wages; this may occur before or after the payment of wages.
- Cashing of payroll checks where the majority of the funds are kept by the employer or are deposited back into the employer's account; this activity may be detected by those financial institutions that have access to paystubs and other payroll records.
- Frequent outbound wire transfers, with no business or apparent lawful purpose, directed to countries at higher risk for human trafficking or to countries that are inconsistent with the customer's expected activity.

- A customer's account appears to function as a funnel account whereby cash deposits occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.
- Multiple, apparently unrelated, customers sending wire transfers to the same beneficiary. These wire senders may also use similar transactional information including, but not limited to, a common address and phone number. When questioned to the extent circumstances allow, the wire senders may have no apparent relation to the recipient of the funds or know the purpose of the wire transfers.
- Transactions conducted by individuals, escorted by a third party (e.g., under the pretext of requiring an interpreter) to transfer funds (that may seem to be their salaries) to other countries.
- Frequent payments to online escort services for advertising, including small posting fees to companies of online classifieds as well as more expensive, higher-end advertising and website hosting companies.
- Frequent transactions, inconsistent with expected activity and/or line of business, carried out by a business customer in apparent efforts to provide sustenance to individuals (e.g., payment for housing, lodging, regular vehicle rentals, purchases of large amounts of food).
- Payments to employment or student recruitment agencies that are not licensed/registered or that have labor violations.
- A customer establishes an account or visits a branch to conduct transactions while escorted by a third party (e.g., under the pretext of requiring an interpreter). The third party escorting the customer may have possession of the customer's ID.
- Common signer(s)/custodian(s) in apparently unrelated business and/or personal accounts; similarly, common information (e.g., address, phone number, employment information) used to open multiple accounts in different names.
- Accounts of foreign workers or students where the employer or employment agency serves as a custodian.
- Unexplained/unjustified lifestyle incommensurate with employment or business line; profits/deposits significantly greater than that of peers in similar professions/business lines.
- Inflows are largely received in cash where substantial cash receipts are inconsistent with the customer's line of business; extensive use of cash to purchase assets and to conduct transactions.

The following two red flags may signal anomalous customer activity; however, they should be applied in tandem with other indicators when determining whether transactions are linked to human trafficking.

- Transactional activity (credits and/or debits) inconsistent with a customer's alleged employment, business or expected activity, or where transactions lack a business or apparent lawful purpose.
- Cash deposits or wire transfers are kept below \$3,000 or \$10,000 in apparent efforts to avoid record keeping or CTR filing requirements, respectively.

## UNUSUAL ACTIVITY INDICATIVE OF POTENTIAL TERRORIST FINANCING

The Egmont Group reviewed 22 terrorist financing cases submitted by financial intelligence units (FIUs) and compiled financial and behavioral indicators that were most frequently observed indicators associated to terrorist financing.

### Behavior indicators

- The parties to the transaction (owner, beneficiary, etc.) being from countries known to support terrorist activities and organizations
- Use of false corporations, including shell companies
- Inclusion of the individual in the United Nations 1267 Sanctions list
- Media reports that the account holder is linked to known terrorist organization or is engaged in terrorist activities
- Beneficial owner of the account is not properly identified
- Use of nominees, trusts, family member or third-party accounts
- Use of false identification
- Abuse of nonprofit organizations

### Indicators linked to financial transactions

- The use of funds by nonprofit organization is not consistent with the purpose for which it was established
- The transaction is not economically justified considering the account holder's business or profession
- A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds
- Transactions that are inconsistent with the account's normal activity
- Deposits were structured below the reporting requirements to avoid detection
- Multiple cash deposits and withdrawals with suspicious references
- Frequent domestic and international ATM activity
- No business rationale or economic justifications for the transactions
- Unusual cash activity in foreign bank accounts
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country
- Use of multiple foreign bank accounts

[illegible]

[illegible]

[illegible]

# Chapter 4

## CONDUCTING AND RESPONDING TO INVESTIGATIONS

**T**his chapter discusses the various channels through which financial institutions may receive information to initiate an investigation and explores the steps they should take to ensure that investigations are conducted thoroughly and effectively.

### **Investigations Initiated by the Financial Institution**

---

#### **Sources of Investigations**

---

Investigations may be initiated from proactive monitoring for potentially suspicious activity as well as reactive measures taken to address regulatory findings, referrals or other recommendations. Common investigation initiators include

- regulatory recommendations or official findings;
- transaction monitoring rules designed to detect potentially suspicious activity;
- referrals from customer-facing employees regarding potentially suspicious activity;
- information obtained from internal hotlines;
- negative media information; and
- receipt of a governmental subpoena or search warrant.

#### **REGULATORY RECOMMENDATIONS OR OFFICIAL FINDINGS**

Financial institutions may initiate investigative efforts based on regulatory findings or recommendations. Such efforts may result in the creation of new ongoing monitoring, or may be one-time reviews to address specific questions or observations. Most importantly, investigations initiated as a result of regulatory findings should be clearly documented and designed to ensure that all aspects of the findings are addressed within the time frame (if any) provided by the issuing body. Moreover, senior

management or higher should be made aware of the items noted from the regulatory review, the status in addressing them and the final disposition to ensure the financial institution appropriately remediates the finding or recommendation.

## **TRANSACTION MONITORING**

Financial institutions should establish a program to regularly monitor transactions to proactively identify potentially suspicious activity. Common approaches to transaction monitoring include the creation of in-house, customizable transaction monitoring rules or engaging a third-party vendor to assist with the development and implementation of automated rules. Financial institutions should use a risk-based approach to transaction monitoring and should consider the size of the institution, products offered and the features of those products when designing transaction monitoring rules.

The institution should also have policies and procedures for monitoring for suspicious activity and should clearly specify the parameters and thresholds that are in place to trigger an investigation. These policies should be regularly reviewed and updated to account for changes and enhancements to the monitoring rules program.

The Wolfsberg Group noted in its 2009 Statement on Monitoring, Screening and Searching that an institution's transaction monitoring framework should be aligned to the risk of its business model, the products and services offered and its customer base, and should be embedded in an institution's AML program. The document additionally discusses types of monitoring, typology reviews and staff training.

Transaction monitoring rules should be reviewed at a regular cadence and tuned accordingly to ensure that they continue to operate as designed. Tuning practices may include evaluating the output of monitoring rules, examining specific thresholds and conducting above and below-the-line testing to determine whether rule adjustments are necessary.

## **REFERRALS FROM CUSTOMER-FACING EMPLOYEES**

In addition to automated, ongoing transaction monitoring, financial institutions may also have a mechanism by which customer-facing employees can refer matters to be investigated for potentially suspicious activity. Depending on the size of the institution, there may be manual referral processes via email or telephone, or an internal reporting system that routes the referrals to the appropriate investigative teams. For example, a financial institution may have a specific internal online form to be completed by branch personnel when they identify unusual activity, such as a customer structuring transactions, currency that contains an odor indicative of controlled substances or inconsistent responses by the customer to questions regarding the source of large cash deposits. Upon completion of the form by the branch, it is delivered to a designated AML/CFT compliance email address. Subsequently, the AML/CFT team reviews the activity during the normal course of its investigations process. The existence of these referral mechanisms and the types of activity that may warrant referrals should be included in employee training programs, especially for those on the first line of defense.

## INTERNAL HOTLINES

Internal hotlines are also known as ethics, compliance or whistleblower hotlines. They allow employees to report a wide range of activity including employee fraud, harassment and discrimination, violations of code of conduct, theft of company property and inappropriate gifts. The hotlines may ask the employee to provide his or her identity but most allow for anonymous reporting. In either case, the financial institution is prohibited from retaliating against the person making a report via the hotline in most jurisdictions, and the financial institution must maintain policies, procedures and processes to confidentially investigate the information provided through the hotline. The size and scale of a financial institution will determine the organizational recipient of the hotline information, such as legal, compliance, human resources or corporate security.

## NEGATIVE MEDIA INFORMATION

Investigations may be initiated in response to notable media stories about a financial institution's customer, how a product is used in the market, a geographic location it serves or a money laundering or terrorist event. Thus, financial institutions should develop a process to receive, review and escalate these types of potentially high priority triggers. It is critical to determine whether the negative information is financially risk-relevant to the financial institution. In some instances, financial institutions may proactively monitor media stories and initiate investigations to determine if a suspicious activity or transaction report (SAR or STR) should be filed or if further actions may be necessary.

### Negative News Example



## RECEIPT OF A GOVERNMENTAL SUBPOENA OR SEARCH WARRANT

Financial institutions may initiate investigations upon receipt of a governmental subpoena or search warrant. In either situation, the financial institution maintains two independent obligations: (1) legally fulfill the requirements of the subpoena or warrant, and (2) determine whether the activity of its customer identified in the subpoena or warrant requires the filing of an STR.

Notably, banking regulatory agencies do not need to use subpoenas or search warrants or other jurisdiction-specific legal mechanisms. Rather, their authority to conduct examinations includes the ability to inspect all books and records of a regulated institution.

## SUBPOENA

Subpoenas are usually issued by grand juries, operating under the purview of a court and empower a law enforcement agency to compel the production of documents and testimony. The documents and testimony are designed to allow the law enforcement agency to investigate suspicious transactions, develop evidence and, ultimately, put together a case for prosecution.

If an institution is served with a subpoena compelling the production of certain documents or an individual related to its customer, the institution should have its senior management and/or counsel review the subpoena. If there are no grounds for contesting the subpoena, the institution should take all appropriate measures to comply with the summons or subpoena on a timely and complete basis. Failure to do so can result in adverse action and penalties for the financial institution. The financial institution should not notify the customer being investigated.

For the production of documents related to governmental requests, an institution should start by identifying an employee with knowledge of the institution's files, who will be in charge of retrieving documents for the institution. A system must be put in place to ensure that all documents are located, whether they be in central files, department files or even individual files. In addition, copies of the same document in different hands should be retrieved. This is important because some copies may have handwritten notes by the employees who received them.

If the government asks the institution to keep certain accounts open, such a request should be obtained in writing under proper letterhead and authority from the government.

### *Case Study*

In March 2010, FinCEN issued a \$143 million civil money penalty to Wachovia Bank, NA for failing to implement an effective AML program reasonably designed to identify and report transactions that exhibited indicia of money laundering or other suspicious activity. FinCEN stated, "criminal or grand jury subpoenas with any indicia of money laundering and/or specified unlawful activity may lead to the reporting of suspicious activity, which has value to law enforcement authorities outside of the subpoena process. The Bank failed to review, in a timely fashion, a backlog of over 6,700 subpoenas for potential impact upon the suspicious activity reporting process." As a result, Wachovia failed to timely file thousands of suspicious activity and currency transaction reports, thus greatly diminishing the value of the reports to both law enforcement and regulatory agencies.

## SEARCH WARRANT

A search warrant is a grant of permission from a court for a law enforcement agency to search certain designated premises and to seize specific categories of items or documents. Generally, the requesting agency is required to establish that probable cause exists that evidence of a crime will be located. The warrant is authorized based on information contained in an affidavit submitted by a law enforcement officer.

When a search warrant is served, it is important that everyone present remain calm. Every employee should know that a search warrant is not usually an open-ended demand. Instead, it gives the law enforcement agents the right to enter the premises and to look for and seize only certain items or documents. A search warrant also does not compel testimony.

When presented with a search warrant, an institution should consider taking the following steps.

- Call the financial institution's in-house or outside counsel and/or designated officer in charge of security, risk management or similar area.
- Review the warrant to understand its scope.
- Ask for and obtain a copy of the warrant.
- Ask for a copy of the affidavit that supports the search warrant. The agents are not obligated to provide a copy of the affidavit, but, if a financial institution is allowed to see the affidavit, the financial institution can learn more about the purpose of the investigation.
- Remain present while the agents make an inventory of all items they seize and remove from the premises. Keep track of the records taken by the agents.
- Ask for a copy of law enforcement's inventory of what it has seized.
- Write down the names and agency affiliations of the agents who conduct the search.

Documents and computer records that are protected by the attorney-client or other legal privilege should be so marked and retained separately from general records. Privileged records should be stored in an area (e.g., a cabinet) marked Attorney-Client Privilege.

If the law enforcement agents want to seize these records, institution representatives may object and suggest, as an alternative, that the records be given to the court for safekeeping. All employees should be trained on how to behave in a search, and someone should be designated to communicate with the agents.

## **ORDERS TO RESTRAIN OR FREEZE ACCOUNTS OR ASSETS**

If the law enforcement agency or a prosecutor obtains a court order to freeze an account or to prevent funds from being withdrawn or moved the institution should obtain a copy of the order and should make every effort to comply. Generally, the order is obtained based on a sworn affidavit, which is sometimes included with the order. If the affidavit is not part of the order, the financial institution can ask to see the affidavit, which should provide clues as to why a customer's information is being requested. Whether law enforcement authorities are obligated to provide the affidavit depends on each country's laws and regulations. In some jurisdictions, freezing orders can also be executed by seizure warrant.

### *Case Study*

On May 9, 2013, the United States issued a seizure warrant for \$2.1 million in accounts held at Wells Fargo Bank in the name of Mutum Sigillum LLC and Mark Karpeles, the owner of Mt. Gox. At the time, Mt. Gox, which operated out of Japan, was the world's largest Bitcoin exchange. According to the warrant, Mt. Gox failed to register as a money services business in accordance with U.S. laws. On May 14, 2013, a U.S. seizure warrant was issued for the contents of a Dwolla account, an online payment processor for e-commerce containing an estimated \$2.9 million. The account was held in the name of Mutum Sigillum LLC at Veridian Credit Union. At that time, consumers could purchase bitcoins by depositing funds with Dwolla, and then the funds were

directed to Mt. Gox for the actual purchase of bitcoins. According to the United States, Mt. Gox and Mutum Sigillum were operating as unlicensed money transmitters and, as a result, seized an estimated \$5 million.

## Conducting the Investigation

---

There are several key steps to conducting an effective financial investigation into potential suspicious activity, including: (a) reviewing internal transactions, information obtained from the customer and other relevant internal documentation; (b) identifying and reviewing external information to understand the customer, related entities and relevant media; (c) contacting business line employees responsible for the account relationship and (d) generating a written report documenting relevant findings.

A financial investigator's main objective is to track the movement of money, whether through a bank, broker-dealer, money services business, casino or other financial institution. Financial institutions have a wealth of information at their fingertips because they are in the business of taking in, paying out, accounting for and recording the movement of money. For example, banks maintain signature cards, which are collected at the opening of an account, account statements, deposit tickets, checks and withdrawal items and credit and debit memorandums. Financial institutions also keep records on loans, cashier's checks, certified checks, traveler's checks and money orders. They exchange currency, cash third-party checks and conduct wire transfers, as do most money services businesses. Financial institutions also keep safe-deposit boxes and issue credit cards. Online-based financial institutions maintain login activity logs, IP addresses and geographical location information.

Often, financial institutions are required to keep records of customer accounts for five years. Although that rule might vary in different countries, it is important for compliance officers at financial institutions to be aware of these legal requirements. Account records and records of other nonaccount activities can be essential to tracking possible money laundering. Other financial institutions keep similar records of transactions and the ability to exert control over an account, such as the ability to trade stocks in a brokerage account.

With all the information financial institutions are privy to, it is important for them to develop and maintain policies and procedures with regard to financial investigations. Typically, financial institutions identify the procedural steps required, the information needed to complete the investigation and any recommended next steps. Here are two examples.

1. An investigation is initiated as a result of a branch teller identifying a new customer that conducted large cash deposits at three different branches on consecutive days just below a statutory cash-reporting threshold. Subsequently, the customer wired 95 percent of the funds to an unrelated individual residing in a high-risk jurisdiction historically known as a gateway for narcotics traffickers. According to the financial institution's investigation policies and procedures, the following must be done: a documented review of the customers' accounts for one year, including all transactions, KYC information and social media searches for any relevant negative media. The report must analyze the information reviewed and determine whether or not an STR should be filed and any additional remedial measures.

2. An investigation results from a transaction monitoring alert that identified large, round-dollar wire transfers from import/export companies with generic names located in high-risk jurisdictions to its commercial customer. The KYC review indicated the customer was engaged in furniture sales through several retail locations. Further, it identified a high volume of incoming check and credit transactions and no incoming wire transfers; however, the customer would originate wire transfers to low-risk jurisdictions to purchase the furniture. This investigation led to contacting the relationship manager for information about the customer's activity to assist with explaining the deviation. If unexplained, the next step in the investigation would be to determine whether such activity warranted an STR filing.

## **UTILIZING THE INTERNET WHEN CONDUCTING FINANCIAL INVESTIGATIONS**

An effective investigation requires that information be sourced both from the information held by the financial institutions and from external sources. Care should be taken to ensure that information found is reliable and verifiable, and the assistance of external specialists sought if necessary. It is critical to be confident about the soundness of the information relied upon during an investigation, especially when it may be the deciding factor in closing an account or terminating a business relationship.

The Internet is increasingly being used to source information as part of internal investigations. A focused approach to searching reliable and reputable sources can provide useful third-party information and additional context to the files held by the financial institution. Combined with a review of internal documents and records, Internet sources can help in providing a full picture of whether further steps are needed to mitigate possible financial crime risks associated with the customer.

Conducting research on the Internet is most effective when there is a clear understanding of what web sources are considered reliable. For example, while social media sites such as Facebook or LinkedIn can be useful to verify some information, blogs or comments placed on these sites may not prove to be as reliable a source about an individual's reputation. Independent websites maintained by independent standards bodies (e.g., FATF, Wolfsberg, OECD and OFAC) and supervisory authorities (national or state-level regulators, corporate registrars, electoral rolls/ registration lists) can provide valuable information concerning regulatory status, sanctions, fines, business activities and broader commercial activities that may be engaged in by the party under investigation. Furthermore, these sources are considered to have a high degree of reliability.

In some countries, court lists, decisions rendered by courts, magistrates, administrative tribunals and professional oversight bodies with disciplinary powers (e.g., law societies) also maintain information which may prove useful sources of information.

When using the Internet for customer reputation information, care must be taken when researching news or quasi-news websites. Steps should always be taken to verify, from more than one source, the accuracy of negative news articles so as to reduce the risk that reliance is placed solely on a writer's opinion. Journalists have their own biases, as do their employers, and these biases may subtly find their way into articles. In addition, in countries where freedom of speech and press are not well established, journalists are not free to write exactly what they would like. This may often take the form of prominently publicizing negative news about someone who is not in favor with the

government (including what may be politically motivated criminal or civil charges) or downplaying negative news about someone in favor with the government. Not all media is eminently corrupt, but sometimes the source has as much at stake as the subject of the news. This is why investigators must take a close look at the source of the news as well as the news itself and why getting multiple sources is important to try to get a fuller sense of the story. Some sources may have limited parts of the whole story, which only comes out when the investigator has additional pieces of information.

When dealing with a country or region that is known to have tighter controls on what is published on the internet and to restrict the amount of information which is publicly accessible, it may be necessary to seek additional assistance. Particularly when dealing with a valuable client that may justify the additional expense, an institution may want to retain the services of a vendor with expertise in this area to verify whether serious adverse information about a customer is in fact supported by independent sources.

**Tips on searching the Internet:** Before searching the Internet, the investigator should prepare a plan, focusing on the topics under investigation and the types of information needed. This will ensure that the work is undertaken in an efficient and focused manner.

The investigator should start with a metasearch using a number of different search engines and then move to specific search engines with different capabilities. From the metasearch, the investigator can also start narrowing the parameters using keywords. The plan devised in advance will help the investigator to select the keywords and areas where greater focus should be applied. For example, if a customer's transaction activity has raised concerns, the search may begin with the customer's personal and professional background, and then focus on the nature of the commercial activities he or she has been undertaking. This will assist the investigator in assessing whether the transactions appear to be consistent with the reasons given by the customer for opening the account and the expected commercial activity he or she proposed to use it for.

There are good tutorials on the web for those who want to improve their search skills. There are also sites that tell you about search engines for professional searchers. The easiest and most effective way to improve your web-searching skills is to read the Help pages of major search engines and to try out their advanced features.

Some tips on search engines are as follows.

- Using multiple search engines is a good idea, because no single engine covers the entire web.
- If you are searching in a foreign country, use a local search engine.
- Use metasearch engines.

An additional step might be accessing a commercial database. Although these databases require the payment of a fee, public record aggregators can be worth the fee, because they cross-reference a huge number of records. Moreover, they may have certain personally identifiable information, such as date of birth or government identification number, that may not be located on the Internet.

### *Case Study*

During regular transaction monitoring of its customers, a bank identified possible anomalies with one customer's transactions. The customer was an MSB who had advised the bank when it opened the account that its core customers would be drawn from Europe and estimated that it

would have 10 to 20 transactions on the account each month. The company undertook an internal investigation. As a result of its Internet search, the investigator discovered that the company was promoting its money transfer services in the Middle East and East Africa, downplaying the need to provide KYC. The bank quickly took steps to freeze and later close the account once it had notified the finance intelligence unit of its findings.

**Search Scenario: Too Much Money.** Take the case of a gas station owner who deposits \$50,000 in cash per week. Is this money laundering? Many people would simply plug the owner's name into Google and consider their due diligence sufficient. A better approach would be to ask: How much cash do gas stations of that size and location typically deposit? This leads to a very different line of inquiry. Internet sources may disclose sources such as marketing studies, commercial valuation sites or businesses for sale that might provide useful clues about the cash flow of comparable gas stations.

The Internet might also reveal useful information about the area where the gas station is located: population statistics, income levels, ethnicity, crime rates and so on. Is it located on a commuting corridor? Are there competitors nearby? Does it have a car wash or a convenience store attached?

By comparing the business with others and examining the context, it becomes possible to argue that there is "...a high level of cash deposits atypical of the expected business profile"—a classic indicator of money laundering.

**Search Scenario: Unknown Business.** This case involves a bank client who was depositing large amounts of cash in his personal account. The bank suspected that its client was operating an unlicensed money remittance service out of the back of his restaurant. It was about to file a suspicious transaction report when the bank realized that it was missing a key piece of information: the name of the client's restaurant. How did the bank solve the mystery? It began by assuming that the client's restaurant was near the bank. Using a simple online telephone directory the bank was able to generate a list of all the restaurants within one mile of the bank.

But which one belonged to the client? The bank needed a way to look up incorporation records for each of the businesses that it had identified. Not wanting to use a commercial service it went to a free online public records provider. Clicking on the jurisdiction and then the link for corporations led the bank to the right government department, where it input the name of each one of the area restaurants until it found one with its customer listed as a director.

This case provides a useful example of the benefits of starting one's investigation and then bringing the focus into more specific areas in order to gain a complete picture about the customer being investigated.

**Search Scenario: Unusual Bank Account Activity.** What technical skills are useful for know your customer and due diligence? We will use this simple scenario to think about how to approach this investigation. You are asked to research a customer named Cynthia Jenkins in Albuquerque, New Mexico. Transaction monitoring raised an alert that Cynthia appeared to be using her account in a way that was inconsistent with what was anticipated when she first opened the account—or maybe the account had been dormant for some time and had suddenly reactivated. Transaction monitoring showed that Cynthia's account had received a significant number of wire transfers from different

parties in the last two weeks. Each transfer was for \$9,900. When Cynthia first opened the account, she stated that it was for “household expenses.” Your first step might be to confirm Cynthia’s identity and search the Internet to determine whether the use of the account appears to be legitimate.

- Is she listed in the telephone directory or on the electoral roll?
- Where does Cynthia live? Is there any evidence that it is used for any commercial activity that could justify the payments received?
- Is she mentioned in any other public records? Try a public records search engine.
- What information does she provide on social media about her occupation, location and so on?
- Is there evidence that someone could be misusing Cynthia’s account? For example, is she elderly or possibly deceased? Could this be a case of identity theft? Imposters often use the Social Security numbers of dead people. In the United States, it is possible to check the Social Security Death Index by searching for Social Security Death Index.

The information obtained from the Internet searches should be complimented by internal documents and records held by the company. Who were the transfers sent from? From what banks? Do the transfers indicate why the monies were paid? Is it possible to check the Internet to see whether there is any information about the payers?

## **STR Decision-Making Process**

---

The decision of whether or not to file a suspicious transaction report (also known as a suspicious activity report or SAR in the United States) often involves weighing the aggravating and mitigating factors arising from the research conducted during the investigative process. Financial institutions should draft procedures that document the factors to consider when determining whether a suspicious transaction report (STR) is appropriate. Properly trained personnel in charge of investigating and reporting suspicious activities should have a clear and concise procedure for escalating their findings to a compliance officer, manager or other staff member with authority to make the filing decision. The final decision should be documented and supported by the reasoning that was used to make the determination. Oftentimes, the reason not to file an STR maintains a similar level of importance as the reason to file an STR.

After the decision to file has been made, the institution should report the activity to its regulatory agency, law enforcement or both as defined by the applicable regulations within its jurisdiction. Many jurisdictions require STRs to be filed within a specific number of days following the discovery of potentially suspicious activity.

In many jurisdictions, it is a requirement to report certain information regarding STRs to senior management and/or the board of directors. This information may be limited to the number of reports filed, the dollar amounts involved and significant trends as observed by compliance personnel. In some cases, if the activity presents a significant or potentially ongoing risk to the institution, the leaders of the institution should be made aware so that high-level decisions can be made regarding potential changes to systems, staffing, products, services or particular relationships maintained by the institution.

## FILING AN STR

The decision to file an STR should be the result of an accumulation of aggravating factors and a lack of mitigating factors in combination with the knowledge of what is expected activity for the institution's client base, product offerings and geographical area of service. The STR filing should include not only the details of the suspicious activity and the related demographics, but also why the institution finds the activity suspicious. The recipient of the STR does not have the intimate knowledge of what is expected activity for a particular institutions, clients and products and will only stand to benefit from the inclusion of this information. In addition, capturing any known typologies identified as part of the review should be added as well.

If, following the investigation, the institution decides that it should file an STR; it should notify the investigators or prosecutors as soon as possible. However, this may not be practical in certain jurisdictions due to the continuous nature of the STR process and the volume of reports being filed by the reporting institution. The establishment of a filing timeline in concert with country guidelines is also critical to avoiding institutional penalties or fines. The failure to file timely reports is often cited in regulatory actions against financial institutions. The AML/CFT officer or designee should keep the management and board apprised of STR filing metrics and any significant issues resulting from those filings, especially items that pose a regulatory or reputational risk to the institution.

## QUALITY ASSURANCE

All financial institutions are required to file timely and complete STRs, and the quality of the STRs can be an indication of the quality of a financial institution's AML/CFT program. Quality and consistency in the STR decision-making process is critical to ensuring the appropriate level of oversight in the investigative process. A quality assurance (QA) review helps to ensure that STR filings are internally consistent, that the right decisions are being made and that high priority matters are identified and escalated to leadership. The larger the scale of the financial institution, its staff and where it may be located, all have an impact on the QA process. As a result, financial institutions that implement a QA process should document the requirements and qualifications of QA reviewers and regularly review the outcome of QA reviews to assess the quality of staff, training requirements and the general health of the program.

## STR FILING OVERSIGHT/ESCALATION

An institution should have robust policies and procedures documenting the appropriate oversight of the investigations process and regulatory reporting requirements. This should include specific actions to be taken, such as escalation to senior management in cases where a customer-facing employee or individual in the AML/CFT chain of command is complicit or willfully blind to suspicious financial activities.

### *Case Study*

In March 2016, the Office of the Comptroller of the Currency (OCC) issued a Consent Order in which it fined Charles Sanders, the former chief compliance officer and chief risk officer of Gibraltar Private Bank and Trust Co. of Coral Gables, \$2,500 for causing the bank to fail to file

SARs. In the order, the OCC indicated the bank's BSA officer had investigated activity related to a Ponzi scheme at the bank and prepared SARs for filing. Mr. Sanders agreed with the content of the reports, but failed to ensure the bank timely filed the reports.

### Case Study

Florida-based attorney Scott Rothstein pleaded guilty in 2009 to operating a \$1.2 billion Ponzi scheme that involved pulling in investors for confidential out-of-court legal settlements that were, in fact, entirely fabricated. The litigants that were supposedly cashing out of structured settlements were said to be involved in sexual harassment and whistle-blower cases that defendants wanted to remain secret. The premise was viable, but Rothstein offered abnormally large returns for that type of investment, in some cases more than 20 percent in 90 days. Rothstein originally maintained accounts at Gibraltar Private Bank & Trust, where he was personally invested, and which was subsequently penalized \$4 million by the Financial Crimes Enforcement Network (FinCEN) in 2016 for Willful Anti-Money Laundering Compliance Violations. The penalty was the result of deficiencies in Gibraltar's systems that caused the bank to miss alerts related to Rothstein's accounts. Rothstein's role as an investor may have played a role in the lack of regulatory filings related to his accounts; he would also go on to allege a Gibraltar vice president assisted him in moving funds between accounts to fend off compliance staff.

Rothstein opened accounts at TD Bank to continue operating the scheme after some investors informed him they preferred dealing with a large institution. He later indicated that he gave his contact at TD Bank cash for his continued facilitation of the scheme, also noting that the individual "handled any and all concerns raised by bank compliance officials about the accounts" linked to the scheme. FinCEN assessed a \$37.5 million civil money penalty against TD Bank, N.A., in September 2013 for failure to file suspicious activity reports related to the massive Ponzi scheme.

## **Closing the Account**

---

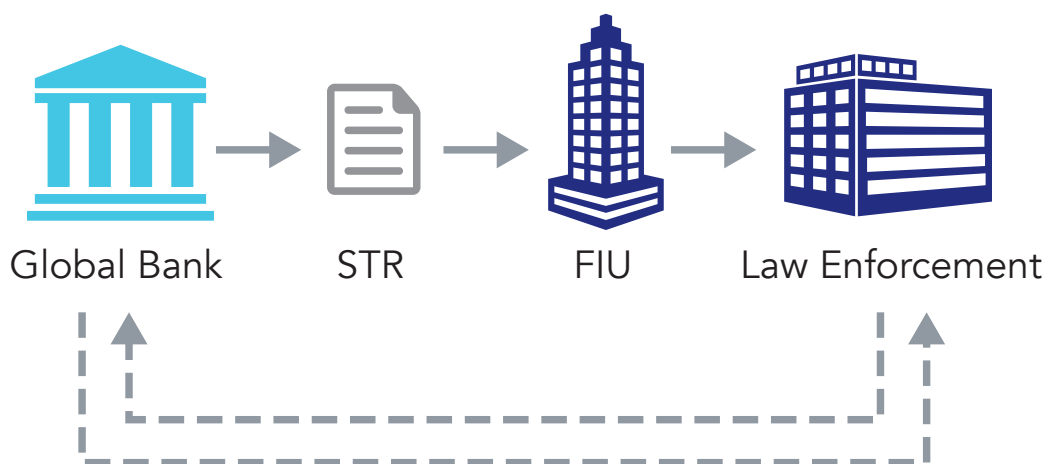
Based on its internal investigation, the financial institution should make an independent determination as to whether to close the account in issue. Some of the factors that the institution should consider are

- the legal basis for closing an account;
- the institution's stated policies and procedures for closing an account, which may include automatic closure recommendation following a specified number of STR filings;
- the seriousness of the underlying conduct. If the conduct rises to the level where the account would ordinarily be closed, then the institution should consider closing the account;
- the reputational risk to the institution posed by maintaining the account; and
- correspondence with law enforcement and requests from law enforcement to either cancel or maintain the account.

## Communicating With Law Enforcement on STRs

When an institution files an STR, the details of that filing may rise to the level that warrants additional law enforcement notification. STRs represent financial intelligence to a country's FIU; depending on the volume of reports filed in a given country a report worthy of priority attention may be hidden in the large number of reports filed. Following the filing of the STR, the responsible compliance officer or designee may decide to contact a particular law enforcement division to notify it of the recent filing to make it aware of activity relevant to its area of coverage or geographical location. Moreover, a law enforcement agent may contact the financial institution that filed the STR seeking the underlying information used in the investigation that resulted in the STR. Therefore, it is critical that each institution develop its own policy and procedures for communicating with law enforcement regarding STRs.

### Communicating With Law Enforcement on STRs Example



## Investigations Initiated by Law Enforcement

Law enforcement agencies may initiate investigations against a financial institution, or contact financial institutions in the context of an investigation involving a customer of the institution. Steps that law enforcement agencies can or should take in conducting a money laundering investigation include the following.

- Follow the money. If the agency is aware of where the laundered money originated or where it ended up, it is appropriate for the agency to attempt to bring the two ends together and to compile a complete understanding of the flow of the funds.

- Leverage the financial knowledge and due diligence information contained in financial institutions. Through information sharing and transactional reviews, a financial institution can assist law enforcement in identifying the originating or ultimate destination of a subject's funds. Furthermore, the supporting documentation that was used to create an STR or customer due diligence file may be used as evidence whereas actual STRs may not be in many jurisdictions.
- Identify the unlawful activity. Most countries define money laundering in terms of predicate offenses or specified unlawful activities. These are usually very extensive and include many felony crimes such as bribery, extortion, racketeering, narcotics trafficking and human trafficking. In order for a money laundering case to result in a conviction, prosecutors need to establish the flow of money as well as the existence of a predicate offense.
- Review databases. FIU databases and commercial databases can provide very useful and extensive financial information and provide leads as to which financial institutions to ask for assistance. Also, records, such as Social Security information in the United States (i.e., tax related information), can be used to further identify subjects.
- Review public records. Court records, as well as corporate filings and credit reports, can provide useful background information.
- Review licensing and registration files. Files, such as records held by motor vehicle departments and other registration databases, can provide background information and useful leads.
- Analyze the financial transactions and account activity of the target. Look for the normal and expected transactions of the individual or entity based on self-disclosures, income and typical flows of funds by similarly situated people. Financial institutions may be able to assist in identifying these items. If the transactions are outside of the norm or stated level of activity, then analyze where the additional funds come from and the composition of the unusual activity.
- Review STRs that might involve any potential individual linked to the target or the transactions or activity.
- In cross-border cases, seek international assistance.

## **Decision to Prosecute a Financial Institution for Money Laundering Violations**

---

When considering whether—or to what extent—to bring a case against an institution involving money laundering-related charges, prosecutors will look at many factors, including the following.

- The institution has a criminal history.
- The institution has cooperated with the investigation.
- The institution discovered and self-reported the money laundering-related issues.
- The institution has had a comprehensive and effective AML/CFT program.
- The institution has taken timely and effective remedial action.
- There are civil remedies available that can serve as punishment.

- Deterring wrongdoing by others is needed and will be served by a prosecution.
- Advice and recommendations from regulatory agencies and/or the FIU for the jurisdiction is available.

Assuming the case is not simple or egregious, the decision to prosecute is frequently determined by what the prosecutors believe was the intent of the institution when it undertook the action in question.

## **Responding to a Law Enforcement Investigation Against a Financial Institution**

---

When a financial institution is confronted with a law enforcement investigation, it should respond quickly and completely to all requests. Failure to do so could cause unnecessary risk or damage to the institution. If a request is overly broad or unduly intrusive, the institution can attempt to narrow the request or can even seek to contest the request, or portions of the request, in court. However, under no circumstances should an institution ignore or delay responding to a law enforcement inquiry or request for documents.

Upon receipt of a law enforcement inquiry, the financial institution needs to ensure that the appropriate senior management is informed and that someone is designated to respond to all law enforcement requests, to monitor the progress of the investigation and to keep senior management, including the board of directors, informed of the nature and progress of the investigation. Of course, reports or information about an investigation should not be provided to any employees, officers or directors of the institution who might be implicated in the investigation.

The financial institution should consider retaining qualified, experienced legal counsel. Such counsel can guide the institution through the inquiry, contest requests that are perceived to be improper and assist in negotiating settlements if necessary.

As set forth below, whenever an institution receives a subpoena, search warrant, or similar law enforcement demand or becomes aware of a government-related investigation involving the institution, it should conduct an inquiry of its own to determine the underlying facts, the institution's exposure and what steps, if any, the institution should take.

## **Monitoring a Law Enforcement Investigation Against a Financial Institution**

---

Financial institutions should ensure that all grand jury subpoenas, as well as other information requests from government agencies, are reviewed by senior management and an investigations group or counsel to determine how best to respond to the inquiry and to determine if the inquiry or the underlying activity might pose a risk to the institution. In addition, the institution should maintain centralized control over all requests and responses to ensure that the requests are responded to on a complete and timely basis and to establish a complete record of what is provided. This centralized record will also assist in the institution's internal investigation.

Vital information can be found in a wide variety of document types, including internal memos, transactional documents, calendars, emails, financial records, travel records, phone logs, signature cards, deposit tickets, checks, withdrawal items, credit and debit memoranda and loan records. Thus, the institution must ensure that relevant documents are not altered, lost or destroyed and that all employees are advised of this fact. This can be done by a memo sent to all relevant employees. However, if there is concern that such a memo might prompt a particular employee to alter or destroy documents, that situation must be dealt with separately.

The institution should also address its document destruction policy to ensure that no documents are destroyed pursuant to that policy during the investigation. It would not be a serious concern if documents relevant to a government investigation were destroyed pursuant to a legitimate policy and prior to obtaining knowledge of the investigation or receiving a subpoena. It could, however, be a serious concern if such documents were destroyed for whatever reason (even pursuant to a legitimate policy) once the institution had been notified about an investigation—even if no subpoena had yet been received.

The institution should ensure the integrity of original documents, while at the same time minimizing disruption to the institution's business. It must ensure that an appropriate system is put in place to organize, maintain, number, secure and copy the documents and to prepare them for production to the government (or to the opposing party in a civil litigation). The documents should be listed in an index so that they can be found when needed.

A detailed privilege log should also be created as the documents are gathered, and privileged documents should be kept separate from other documents to help avoid inadvertent disclosure.

## **Cooperating With Law Enforcement During an Investigation Against a Financial Institution**

---

Providing investigators with the information they need to reach an investigative conclusion may be the most effective way to terminate the investigation before it has a devastating effect on the resources and reputation of the institution. Cooperation may include making employees, including corporate officers, available for interviews, and producing documents without the requirement of a subpoena. It may also include a voluntary disclosure by providing investigators with any report written by counsel regarding the subject under investigation.

The institution should make every effort to stay on good terms with the investigators and prosecutors. At a minimum, a good working relationship will help the institution conduct an effective parallel internal investigation and thereby position the institution to respond more effectively to investigative or prosecutorial inquiries.

It is also important for the institution to try to learn how the investigators and prosecutors view the facts. If they happen to be wrong about some of the facts, the institution will have an opportunity to rectify the situation. At a minimum, if the institution is aware of the investigators' and prosecutors' concerns, it will be in a better position to respond to them.

## **Obtaining Counsel for an Investigation Against a Financial Institution**

---

### **RETAINING COUNSEL**

With regard to particularly large, important or serious investigations, it may be appropriate for the institution to retain counsel to assist in responding to the investigation or advising the institution during the course of the investigation. Many financial institutions, such as large banks and securities dealers, have legal counsel on their staff. But many other financial institutions, such as small money services businesses, do not ordinarily have legal counsel on their payroll. In either case, it is recommended that institutions hire or consult experienced outside legal counsel if confronted with a government investigation of the institution itself. If the institution is actually facing imminent criminal prosecution or indictment, it needs an experienced attorney who specializes in defending financial institutions in these matters.

Using in-house counsel will, of course, cost less, and in-house counsel will start out with a better knowledge of the institution, its personnel, its policies and procedures. However, if the conduct under investigation could involve or lead to a criminal investigation or indictment, outside counsel may be more appropriate.

If the institution determines that it is appropriate to involve counsel, in-house or outside, it should take appropriate measures to ensure that the counsel is sufficiently experienced and knowledgeable with regard to the factual and legal issues involved. In addition, the institution should determine the nature and scope of the role of counsel and should ensure that senior management is aware of and supports the involvement of counsel.

### **ATTORNEY-CLIENT PRIVILEGE APPLIED TO ENTITIES AND INDIVIDUALS**

In an internal investigation, all parties should be aware that attorneys for the organization represent the entity and not its employees. Counsel should understand these issues and should conduct the internal investigation accordingly. Work product and communications may be protected under attorney-client privilege. There may be major consequences if the interests of an entity and its employees diverge or conflict, or if an employee could implicate the employer or vice versa. In such cases, separate counsel may be required.

### **DISSEMINATION OF A WRITTEN REPORT BY COUNSEL**

If counsel for the institution prepares a written report of an investigation, the institution should take steps to not inadvertently waive the attorney-client privilege by distributing the report to people who should not receive it. Every page of the report should contain a statement that it is confidential and is subject to the attorney-client privilege and work-product privilege.

Copies of the report should be numbered and a list of people who are given copies to read should be maintained. After a set period of time, all copies should be returned. Persons obtaining the report should be instructed not to make notes on their copies. All copies should be maintained in a file separate from regular institution files in a further effort to maintain the highest level of protection.

## **Notices to Employees as a Result of an Investigation Against a Financial Institution**

---

With regard to investigations conducted by the government, employees should be informed of the investigation and should be instructed not to produce corporate documents directly. Rather, they should inform senior management or counsel of all requests for documentation and provide the documents to them for production. In that way, the institution will know what is being requested and what has been produced. In addition, the institution can determine what, if any, requests should be contested. The same procedure should be followed with regard to requests for employee interviews.

## **Interviewing Employees as a Result of a Law Enforcement Investigation Against a Financial Institution**

---

In addition to securing and reviewing all relevant documentation, it is important to interview all knowledgeable employees. These employees should be interviewed as soon as practicable so that their memories are the freshest and so that they can direct management or counsel to relevant documents and people on a timely basis.

In addition, the institution, usually counsel, should prepare employees who expect to be interviewed by law enforcement investigators and should debrief them after their interviews. The former will help the employee to understand how to handle the process and the latter will assist the institution in better understanding the scope and direction of the government investigation. As stated above, all requests for employee interviews by law enforcement investigators should go through a single person or centralized location.

Most employees are not accustomed or comfortable with being interviewed—either by law enforcement investigators or counsel for the institution. Therefore, care should be given to put them at ease to the extent possible.

It is also helpful to have interviews as noncontentious as possible. Background and open-ended questions should be used at the beginning of the interview, together with a nonconfrontational review of documents. More contentious questions, if necessary, should be held off for later.

## **Media Relations**

---

People often mistakenly overlook the importance of public and media relations in defending an organization. Public perception is vital to the organization's success in maintaining public trust. If the facts are not on the institution's side, "no comment" may be the best response it can offer. Misleading or false statements that attempt to indicate that the institution has no problems and have done nothing wrong can worsen the situation. When such statements are made by a publicly traded company, they can invite additional scrutiny by regulatory and law enforcement agencies.

### *Case Study*

When a financial institution under investigation by U.S. authorities cooperates, it oftentimes may result in a deference of prosecution of the financial institution, reduced penalties or the removal of ongoing regulatory review specific to the action to the satisfaction of authorities. On August 6, 2007, American Express Bank International (AEBI) agreed to a fine of \$65 million with U.S. authorities and a deferred prosecution agreement with the U.S. Department of Justice for failing to maintain an effective AML/CFT program related to significant deficiencies in detecting and reporting black market peso exchange (BMPE) transactions. At that time, a spokesperson from AEBI stated, “We have cooperated fully with the government and understand the need for absolute vigilance in our efforts to protect against money laundering. We have already made substantial efforts to augment and strengthen our compliance programs and will continue to do so. We are firmly committed to the agreements we have reached and to conducting our business with the highest standards of integrity, compliance and control.”

## AML/CFT Cooperation Between Countries

---

### FATF Recommendations on Cooperation Between Countries

---

Practices that restrict international cooperation between supervisory authorities or financial intelligence units in analyzing and investigating suspicious transactions or money laundering crimes, confiscating assets or extraditing accused money launderers are serious obstacles to combating money laundering.

Recommendations 36 through 40 of FATF's 40 Recommendations on establishing and maintaining effective AML/CFT programs pertain specifically to the international aspects of money laundering and terrorist financing investigations. They deal with mutual legal assistance treaties, extradition, confiscation of assets and mechanisms to exchange information internationally.

### International Money Laundering Information Network

---

The International Money Laundering Information Network (IMoLIN) serves as a clearinghouse of money laundering information for the benefit of national and international anti-money laundering agencies. It was developed and is administered by the Global Program against Money Laundering of the United Nations Office on Drugs and Crimes (UNODC) on behalf of the U.N. and other international organizations, including Interpol. IMoLIN has five main features, all but one accessible to the public.

- **AMLID:** Anti-Money Laundering International Database—A compendium and analysis of national AML laws and regulations, as well as information on national contacts and authorities. The database is password protected.
- **Reference data:** Research and analysis, bibliography, conventions, legal instruments and model laws.

- **Country page:** Includes full text of AML legislation where available, and links to national FIUs.
- **Calendar of events:** Chronological listing of training events, conferences, seminars, workshops and other meetings in the AML field.
- **Current events:** Current news of recent AML initiatives.

## Mutual Legal Assistance Treaties

---

If evidence is required from another jurisdiction, a request can be made for mutual legal assistance. Mutual legal assistance treaties (MLATs) provide a legal basis for transmitting evidence that can be used for prosecution and judicial proceedings.

As an example, the Treaty Between Canada and the Kingdom of Spain on Mutual Assistance in Criminal Matters, which has been in force since March 3, 1995, defines criminal matters as “investigations or proceedings relating to offenses concerning taxation, duties, customs and international transfer of capital or payments.” Moreover, it defines assistance as the “taking of evidence and obtaining of statements of persons; provision of information, documents and other records, including criminal records, judicial records and government records; location of persons and objects, including their identification; search and seizure; delivery of property, including lending of exhibits; making detained persons and others available to give evidence or assist investigations; service of documents, including documents seeking the attendance of persons; measures to locate, restrain and forfeit the proceeds of crime; and other assistance consistent with the objects of this Treaty.”

Procedures can vary but the typical process is outlined below.

- The central authority of the requesting country sends a *commission rogatoire* (letters rogatory, or letter of request) to the central authority of the other country. The letter includes the information sought, the nature of the request, the criminal charges in the requesting country and the legal provision under which the request is made.
- The central authority that receives the request sends it to a local financial investigator to find out if the information is available.
- An investigator from the requesting country then visits the country where the information is sought and accompanies the local investigator during visits or when statements are taken.
- The investigator asks the central authority for permission to remove the evidence to the requesting country.
- The central authority sends the evidence to the requesting central authority, thereby satisfying the request for mutual legal assistance. Local witnesses may need to attend court hearings in the requesting country.

## Financial Intelligence Units

Financial intelligence units (FIUs) are mandatory national agencies that handle financial intelligence. FIUs are agencies that receive reports of suspicious transactions from financial institutions and other people and entities, analyze them and disseminate the resulting intelligence to local law enforcement agencies and foreign FIUs to combat money laundering.

The first FIUs were established in the early 1990s in response to the need for a central agency to receive, analyze and disseminate financial information to combat money laundering. The number of FIUs has now increased to the point where the Egmont Group, the informal international association of FIUs, has more than 150 members.

The European FIUs established in the late 90s were predominantly domestically organized and focused. However, to fight the threat posed by criminals and terrorists exploiting the open borders of the EU, the FIUs of Luxembourg, UK, Italy and France, joined the Dutch FIU with its initiative to create a decentralized network for the FIUs to exchange information in a more sophisticated way. With the start of the pilot project in 2004, FIU.net was born. Starting in 2006, the former Directorate-General Justice, Freedom and Security (DG JLS), later Directorate-General for Migration and Home Affairs (DG HOME) of the European Commission, the Dutch Ministry of Security and Justice together with the participating FIUs funded the EU FIU.net Project that lasted a decade.

In that period the FIU.net Bureau and the project support team together with the FIUs, developed the FIU.net system into a sophisticated, effective tool in the fight against money laundering and terrorist financing. During those years, they added features to FIU.net like Ma3tch, a revolutionary way to match and detect common subjects without having to expose information that is not relevant to others, and the Templates feature, which made it easy to adjust the system to specific needs of an individual FIU and so on.

In 2012, FATF adopted a revised set of recommendations on combating money laundering that, for the first time, included explicit recommendations for the establishment and functioning of FIUs. Although the FIU members of the Egmont Group share the same core functions of receiving, analyzing and disseminating financial information to combat money laundering and financing of terrorism, they often differ in how they are established and how they function. In 2016, the European Union initiated a number of measures to strengthen the role of FIUs and their ability to share information across Europe as part of its comprehensive action plan towards the fight against terrorism.

### Three Basic Functions of an FIU



FIUs play an important role in the AML/CFT framework. Recommendation 29 of the 2012 FATF Recommendations states that countries should establish a financial intelligence unit (FIU) that serves as a national center for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offenses and terrorist financing and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

Articles 30 and 31 of the Recommendations outline the powers that the FIU and other competent authorities responsible for conducting investigations. These include

1. responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies;
2. at least in all cases related to major proceeds-generating offenses, developing a proactive parallel financial investigation when pursuing money laundering, associated predicate offenses and terrorist financing, including cases where the associated predicate offense occurs outside their jurisdictions;
3. expeditiously identifying, tracing and initiating actions to freeze and seize property that is or may become subject to confiscation, or is suspected of being proceeds of crime;
4. access to all necessary documents and information for use in those investigations and in prosecutions and related actions; this should include powers to use compulsory measures for the production of records held by financial institutions, designated nonfinancial businesses and professionals (DNFBPs) and other natural or legal persons for the search of people and premises, for taking witness statements and for the seizure and obtaining of evidence; and
5. using a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offenses and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery.

The Australian Transaction Reports and Analysis Centre (AUSTRAC), founded in 1989, is Australia's primary source for financial intelligence used to fight serious and organized crime and terrorism financing. In the UK, its FIU is part of the National Crime Agency (NCA). The NCA became operational in 2013 and leads UK law enforcement's fight against serious and organized crime. In the U.S., FinCEN was established in 1990 with a mission to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis and dissemination of financial intelligence and strategic use of financial authorities.

The FIUs, with the task of receiving and analyzing suspicious transaction reports and maintaining close links with police and customs authorities, share information among themselves informally in the context of investigations, usually on the basis of memoranda of understanding (MOU). The Egmont Group of FIUs has established a model for such MOUs. Unlike the MLAT, this gateway is not ordinarily used for obtaining evidence, but for obtaining intelligence that might lead to evidence.

In June 2001, the members adopted, “Principles of Information Exchange Between Financial Intelligence Units,” and incorporated the document into its Statement of Purpose. Some countries may restrict the exchange of information with other FIUs or the access to information requested by an FIU. This document describes practices that maximize cooperation between FIUs and can be useful to government authorities when considering anti-money laundering legislation.

Furthermore, to address practical issues that impede mutual assistance, the document provides best practices for the exchange of information between FIUs. When dealing with international information requests, FIUs are urged to take these best practices into account.

Here are some principles included in the document.

- The Egmont principle of free exchange of information at the FIU level should be possible on the basis of reciprocity, including spontaneous exchange.
- Differences in the definition of offenses that fall under the competence of FIUs should not be an obstacle to free exchange of information at the FIU level. To this end, the FIU’s competence should extend to all predicate offenses for money laundering, as well as terrorist financing.
- The exchange of information between FIUs should take place as informally and as rapidly as possible and with no excessive formal prerequisites, while guaranteeing protection of privacy and confidentiality of the shared data.
- Should an FIU still need a memorandum of understanding to exchange information, it should be negotiated and signed by the FIU without undue delay. To that end, the FIU should have the authority to sign MOUs independently.
- It should be possible for communication between FIUs to take place directly, without intermediaries.
- Providing an FIU’s consent to disseminate the information for law enforcement or judicial purposes should be granted promptly and to the greatest extent possible. The FIU providing the information should not deny permission to disseminate the information unless doing so would fall beyond the scope of its AML/CFT provisions, could impair a criminal investigation, would be clearly disproportionate to the legitimate interests of an individual or legal person or the country of the providing FIU or would otherwise not be in accord with basic principles of national law. Any refusal to grant consent should be appropriately explained.

The following practices should be observed by the FIU requesting the information.

- All FIUs should submit requests for information in compliance with the Principles for Information Exchange set out by the Egmont Group. Where applicable, the provisions of information-sharing arrangements between FIUs should also be observed.
- Requests for information should be submitted as soon as the precise assistance required is identified.
- When an FIU has information that might be useful to another FIU, it should consider supplying it spontaneously as soon as the relevance of sharing this information is identified.

- The exchange of information between Egmont FIUs should take place in a secure way. To this end, the Egmont FIUs should use the Egmont Secure Web (ESW) where appropriate.

An example of FIUs collaborating and utilizing MOUs was in October 2013, when FinCEN and Mexico's National Banking and Securities Commission (CNBV) executed the first-ever MOU to facilitate the exchange of supervisory information in support of both agencies' AML/CFT missions. Moreover, it provided for strict controls and safeguards to ensure that shared information is well protected and used in a confidential and authorized manner for AML/CFT supervision purposes only.

**NOTES:**

[illegible]



# Chapter 5

## Glossary of Terms

### A

---

**Affidavit**

A written statement given under oath before an officer of the court, notary public or other authorized person. It is commonly used as the factual basis for an application for a search, arrest or seizure warrant.

**Alternative remittance system (ARS)**

Underground banking or informal value transfer systems (IVTS). Often associated with ethnic groups from the Middle East, Africa or Asia, and commonly involves the transfer of values among countries outside of the formal banking system. The remittance entity can be an ordinary shop selling goods that has an arrangement with a correspondent business in another country. There is usually no physical movement of currency and a lack of formality with regard to verification and record keeping. The money transfer takes place by coded information that is passed through chits, couriers, letters, faxes, emails, text messages or online chat systems, followed by some form of telecommunications confirmations.

**Anti-Money Laundering International Database (AMLID)**

A compendium of analyses of anti-money laundering laws and regulations, including two general classes of money laundering control measures—domestic laws and international cooperation—as well as information on national contacts and authorities. A secure, multilingual database, AMLID is an important reference tool for law enforcement officers involved in cross-jurisdictional work.

**Anti-money laundering program**

The system designed to assist institutions in their fight against money laundering and terrorist financing. In many jurisdictions, government regulations require financial institutions, including banks, securities dealers and money services businesses, to establish such programs. At a minimum, the anti-money laundering program should include

1. written internal policies, procedures and controls;
2. a designated AML compliance officer;
3. ongoing employee training and
4. independent review to test the program

**Anti-money laundering and counter-financing of terrorism program**

*See anti-money laundering program*

**Arrest warrant**

A court order directing a law enforcement officer to seize and detain a particular person and require him or her to provide an answer to a complaint or otherwise appear in court.

**Asia/Pacific Group on Money Laundering (APG)**

A Financial Action Task Force (FATF)-style regional body consisting of jurisdictions in the Asia/Pacific Region.

**Asset protection**

A process that includes reorganizing how assets are held in order to make them less vulnerable should a claim be made against a person. Asset protection is also a term used by tax planners for measures taken to protect assets from taxation in other jurisdictions.

**Asset protection trusts (APTs)**

A special form of irrevocable trust usually created (i.e., settled) offshore for the principal purposes of preserving and protecting part of one's wealth from creditors. Title to the asset is transferred to a person named the trustee. APTs are generally used for asset protection and are usually tax neutral. Their ultimate function is to provide for the beneficiaries. Some proponents advertise APTs as allowing foreign trustees to ignore U.S. court orders and to simply transfer the trust to another jurisdiction in response to legal action threatening the trust's assets.

**Automated Clearing House (ACH)**

An electronic banking network that processes large volumes of both credit and debit transactions that originate in batches. ACH credit transfers include direct deposit payroll payments and payments to contractors and vendors. ACH debit transfers include consumer payments on insurance premiums, mortgage loans and other kinds of expenses.

**Automated teller machine (ATM)**

An electronic banking outlet that allows customers to complete basic transactions without the assistance of a bank employee. ATMs generally dispense cash, allow check and cash deposits and transfers to be made, as well as balance inquiries.

---

# B

---

**Bank draft**

Vulnerable to money laundering because it represents a reputable international monetary instrument drawn on a reputable institution, and is often made payable—in cash—upon presentation and at the issuing institution's account in another country.

**Bank secrecy**

Refers to laws and regulations in countries that prohibit banks from disclosing information about an account—or even revealing its existence—without the consent of the account holder. Impedes the flow of information across national borders among financial institutions and their supervisors. One of FATF's 40 Recommendations states that countries should ensure that secrecy laws do not inhibit the implementation of the FATF Recommendations.

**Bank Secrecy Act (BSA)**

The primary U.S. anti-money laundering regulatory statute (Title 31, U.S. Code Sections 5311-5355) enacted in 1970 and most notably amended by the USA PATRIOT Act in 2001. Among other measures, it imposes money laundering controls on financial institutions and many other businesses, including the requirement to report and to keep records of various financial transactions.

**Bank Secrecy Act (BSA) compliance program**

A program that U.S.-based financial institutions—as defined by the Bank Secrecy Act—are required to establish and implement in order to control money laundering and related financial crimes. The program's components include at a minimum: the development of internal policies, procedures and controls; the designation of a compliance officer; ongoing employee training and an independent audit function to test the program.

**Basel Committee on Banking Supervision (Basel Committee)**

The Basel Committee was established by the G-10's central bank of governors in 1974 to promote sound supervisory standards worldwide. Its Secretariat is appointed by the Bank for International Settlements in Basel, Switzerland. It has issued, among others, papers on customer due diligence for banks, consolidated KYC risk management, transparency in payment messages, due diligence and transparency regarding cover payment messages related to cross-border wire transfers and sharing of financial records among jurisdictions in connection with the fight against terrorist financing. *See [www.bis.org/bcbs](http://www.bis.org/bcbs).*

**Batch processing**

A type of data processing and data communications transmission in which related transactions are grouped together and transmitted for processing, usually by the same computer and under the same application.

**Bearer form**

In relation to a certificate, share transfer or other document, a bearer form enables a designated investment or deposit to be sold, transferred, surrendered or addressed to a bearer without the need to obtain further written instructions.

**Bearer negotiable instruments**

Includes monetary instruments in bearer form such as: negotiable instruments (including checks, promissory notes and money orders) that are either in bearer form, are endorsed without restriction, are made out to a payee or are otherwise in such form that title thereto passes upon delivery.

**Bearer share**

Negotiable instruments that accord ownership in a corporation to the person who is in physical possession of the bearer share certificate, a certificate made out to Bearer and not in the name of an individual or organization.

**Benami account**

Also called a nominee account. Held by one person or entity on behalf of another or others, Benami accounts are associated with the hawala underground banking system of the Indian subcontinent. A person in one jurisdiction seeking to move funds through a hawaladar to another jurisdiction may use a Benami account or Benami transaction to disguise his or her true identity or the identity of the recipient of the funds.

**Beneficial owner**

The term beneficial owner has two different definitions depending on the context.

- The natural person who ultimately owns or controls an account through which a transaction is being conducted.
- The natural people who have significant ownership of, as well as those who exercise ultimate effective control over, a legal person or arrangement.

**Beneficiary**

The term beneficiary has two different definitions depending on the context.

- The person (natural or legal) who benefits from a transaction, such as the party receiving the proceeds of a wire, a payout on an insurance policy.
- In the trust context, all trusts (other than charitable or statutory-permitted noncharitable trusts) must have beneficiaries, which may include the settlor. Trusts must also include a maximum time frame, known as the perpetuity period, which normally extends up to 100 years. Although trusts must always have some ultimately ascertainable beneficiary, they may have no defined existing beneficiaries.

**Bill stuffing**

A casino customer goes to various slot machines putting cash in the bill acceptors and collects cash-out tickets with nominal gaming activity, then cashes out at the casino cage or asks for a check.

**Black Market Peso Exchange (BMPE)**

The Black Market Peso Exchange (BMPE) is an example of a complex method of trade-based money laundering. The BMPE originally was driven by Colombia's restrictive policies on currency exchange. To circumvent those policies, Colombian businesses bypassed the government levies by dealing with peso brokers that dealt in the black market or parallel financial market. Colombian drug traffickers took advantage of this method to receive Colombian pesos in Colombia in exchange for U.S. drug dollars located in the U.S.

# C

---

**Cardholder**

Person to whom a financial transaction card is issued, or an additional person authorized to use the card.

**Caribbean Financial Action Task Force (CFATF)**

An FATF-style regional body comprising Caribbean nations, including Aruba, the Bahamas, the British Virgin Islands, the Cayman Islands and Jamaica.

**Casa de cambio**

Also called a bureau de change or an exchange office, a casa de cambio offers a range of services that are attractive to money launderers: currency exchange and consolidation of small denomination bank notes into larger ones; exchange of financial instruments such as travelers checks, money orders and personal checks; and telegraphic transfer facilities.

**Cash-intensive business**

Any business in which customers usually pay with cash for the products or services provided, such as restaurants, pizza delivery services, taxi firms, coin-operated machines or car washes. Some money launderers run or use cash-based businesses to commingle illegally obtained funds with cash actually generated by the business.

**Cash collateralized loans**

A cash collateralized loan has cash deposits as the loan's collateral. The cash deposits can sometimes reside in another jurisdiction.

**Cash deposits**

Sums of currency deposited in one or more accounts at a financial institution. Vulnerable to money laundering in the placement phase, as criminals move their cash into the noncash economy by making deposits into accounts at financial institutions.

**Cashier's check**

Common monetary instrument often purchased with cash. Can be used for laundering purposes, cashier's checks provide an instrument drawn on a financial institution.

**CICAD (Spanish: Comisión Interamericana para el Control del Abuso de Drogas)**

*See Organization of American States—Inter-American Drug Abuse Control Commission.*

**Collection accounts**

Immigrants from foreign countries deposit many small amounts of currency into one account where they reside, and the collected sum is transferred to an account in their home country without documentation of the sources of the funds. Certain ethnic groups from Asia or Africa may use collection accounts to launder money.

**Commission rogatoire**

Also known as letters rogatory, a commission rogatoire is a written request for legal or judicial assistance sent by the central authority of one country to the central authority of another when seeking evidence from the foreign jurisdiction. The letter typically specifies the nature of the request, the relevant criminal charges in the requesting country, the legal provision under which the request is made, and the information sought.

**Concentration account**

Also called an omnibus account. Held by a financial institution in its name, a concentration account is used primarily for internal administrative or bank-to-bank transactions in which funds are transmitted and commingled without personally identifying the originators.

**Concentration risk**

Concentration risk primarily applies to the asset side of the balance sheet. As a common practice, supervisory authorities not only require financial institutions to have information systems to identify credit concentrations, but also set limits to restrict bank exposure to single borrowers or groups of related borrowers. On the liability side, concentration risk is associated with funding risk, especially the risk of early and sudden withdrawal of funds by large depositors that could harm an institution's liquidity.

**Confidentiality**

Keeping certain facts, data and information out of public or unauthorized view. In most jurisdictions, confidentiality is required when filing suspicious transaction or activity reports—the filing institution's employees cannot notify a customer that a report has been filed. In another context, a breach of confidentiality can occur when an institution discloses client information to enforcement agencies or a financial intelligence unit in violation of the jurisdiction's bank secrecy laws.

**Confiscation**

Includes forfeiture where applicable, and means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to the state. Upon transfer, the individual(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture lose all rights, in principle, to the confiscated or forfeited assets.

**Corporate vehicles**

Types of legal entities that may be subject to misuse such as private limited companies and public limited companies whose shares are not traded on a stock exchange, trusts, nonprofit organizations, limited partnerships and limited liability partnerships and private investment companies. Occasionally, it is difficult to identify the people who are the ultimate beneficial owners and controllers of corporate vehicles, which makes the vehicles vulnerable to money laundering.

**Correspondent banking**

The provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Large international banks typically act as correspondents for hundreds of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers of funds, check clearing services, payable-through accounts and foreign exchange services.

**Credit cards**

A plastic card with a credit limit used to purchase goods and services and to obtain cash advances on credit. The cardholder is subsequently billed by the issuer for repayment of the credit extended. Credit cards may be used to launder money when payments of the amounts owed on the card are made with criminal money.

**Criminal proceeds**

Any property derived from or obtained, directly or indirectly, through the commission of a crime.

**Cross border**

Used in the context of activities that involve at least two countries, such as wiring money from one country to another or taking currency across a border.

**Currency**

Banknotes and coins that are in circulation as a medium of exchange.

**Currency smuggling**

The illicit movement of large quantities of cash across borders, often into countries without strict banking secrecy, poor exchange controls or poor anti-money laundering legislation.

**Currency transaction report (CTR)**

A report that documents a physical currency transaction that exceeds a certain monetary threshold. A CTR can also be filed on multiple currency transactions that occur in one day exceeding the required reporting amount. Some countries, including the U.S., have requirements addressing when CTRs should be filed with government authorities.

**Custodian**

A bank, financial institution or other entity that is responsible for managing, administering or safekeeping assets for other people or institutions. A custodian holds assets to minimize risk of theft or loss, and does not actively trade or handle the assets.

**Custody**

The act of or authority to safeguard and administer clients' investments or assets.

**Customer due diligence (CDD)**

In terms of money laundering controls, CDD requires policies, practices and procedures that enable a financial institution to predict with relative certainty the types of transactions in which the customer is likely to engage. CDD includes not only establishing the identity of customers, but also establishing a baseline of account activity to identify those transactions that do not conform to normal or expected transactions.

---

# D

---

**Debit card**

A card that permits an account holder to draw funds from an existing account. Debit cards are used to pay obligations or make purchases. Debit cards can be used in a variety of places, including on the Internet. Debit cards often allow for movement of cash via cash-back transactions or withdrawals at ATMs.

**Designated Categories of Offense**

Those crimes considered by FATF to be money-laundering predicate offenses. Each country can separately decide how it will define specific offenses and their elements under its own domestic laws. Many nations do not specify which crimes can serve as predicates for laundering prosecutions and merely state that all serious felonies may be predicates.

**Designated nonfinancial businesses and professions**

FATF recommends certain standards apply to nonfinancial businesses and professions, including specifically

- casinos (including Internet casinos);
- real estate agents;
- dealers in precious metals and precious stones;
- lawyers, notaries, other independent legal professionals and accountants (Refers to those who prepare or carry out certain duties on behalf of clients); and
- trust and company service providers who prepare or carry out certain duties on behalf of their clients.

**Domestic transfer**

Electronic funds transfer in which the originator and beneficiary institutions are located in the same jurisdiction. A domestic transfer therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the actual system used to send the wire transfer may be located in another jurisdiction or online.

---

# E

---

**Eastern and Southern African Anti-Money Laundering Group (ESAAMLG)**

An FATF-style regional body comprising countries from the Eastern region of Africa down to the Southern tip of Africa, established in 1999.

**Egmont Group of Financial Intelligence Units**

The Egmont Group consists of numerous national financial intelligence units (FIUs) that meet regularly to find ways to promote the development of FIUs and to cooperate, especially in the area of information exchange, training and the sharing of expertise. The goal of the group is to provide a forum for FIUs to improve cooperation in the fight against money laundering and the financing of terrorism, and to foster the implementation of domestic programs in this field.

**Electronic funds transfer (EFT)**

The movement of funds between financial institutions electronically. The two most common electronic funds transfer systems in the U.S. are FedWire and CHIPS. (SWIFT is often referred to as the third EFT system, but in reality it is an international messaging system that carries instructions for wire transfers between institutions, rather than the wire transfer system itself.)

**Electronic money (emoney)**

Electronic cash represents a series of monetary value units in some electronic format, such as being stored electronically online, on the hard drive of a device or on the microchip of a plastic card.

**Enhanced due diligence (EDD)**

In conjunction with customer due diligence, EDD calls for additional measures aimed at identifying and mitigating the risk posed by higher risk customers. It requires developing a more thorough knowledge of the nature of the customer, the customer's business and understanding of the transactions in the account than a standard or lower risk customer. A financial institution should ensure account profiles are current and monitoring should be risk-based.

**Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)**

An FATF-style regional body formed in October 2004 in Moscow.

**European Union (EU)**

The modern EU was founded in the Treaty of Maastricht on European Union, signed in 1992 and effective in 1993. The EU is a politico-economic union of member states located primarily in Europe. Member states have set up three common institutions (the European Parliament, the European Commission and the Council of the European Union) to which they delegate part of their sovereignty so that decisions on specific matters of collective interest can be made democratically at the European level. As a result, people, goods, services and money flow freely through the EU.

**European Union Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing**

First adopted by the European Union in June 1991 and updated in 1997, 2005 and 2015, the Directive requires EU member states to ensure that money laundering and terrorist financing are prohibited. The Directive applies to a broad spectrum of entities, including financial institutions, accountants, notaries, trust companies, estate agents and some providers of gambling services. Member states are expected to identify and mitigate risks appropriately. They are to oversee financial institutions and other obliged entities, including establishing standards for customer due diligence, prohibition of shell banking relationships, establishing FIUs, developing standards for document retention and requiring consequences for failure to comply.

**Europol**

Europol is the EU's law enforcement agency. Its main goal is to help achieve a safer Europe for the benefit of all EU citizens. In the area of anti-money laundering, Europol provides member states' law enforcement authorities with operational and analytical support via the Europol liaison officers (ELOs) and its analysts, as well as state-of-the-art databases and communication channels.

**Express trust**

A trust created expressly by the settlor, usually in the form of a document such as a written deed of trust. An express trust differs from trusts that do not result from the specific intent or decision of a settlor to create a trust (e.g., constructive trust established by a court of law to address undeclared property).

**Extradition**

The surrender by one jurisdiction to another of an accused or convicted person under an agreement that specifies the terms of such exchanges.

**Extraterritorial reach**

The extension of one country's policies and laws to the citizens and institutions of another. Depending on jurisdiction, money laundering laws may extend prohibitions and sanctions into other jurisdictions.

---

# F

---

**Financial Action Task Force (FATF)**

FATF was chartered in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policy making body that sets anti-money laundering standards and counter-terrorist financing measures worldwide. Its Recommendations do not have the force of law. Thirty-five countries and two international organizations are members. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. FATF develops annual typology reports showcasing current money laundering and terrorist financing trends and methods. *See [www.fatf-gafi.org](http://www.fatf-gafi.org).*

**Financial Action Task Force on Money Laundering in Latin America (GAFILAT)**

An FATF-style regional body for Latin America, established in 2000.

**Financial Action Task Force-Style Regional Body (FSRB)**

FSRBs have forms and functions similar to those of FATF. However, their efforts are targeted to specific regions. In conjunction with FATF, FSRBs constitute an affiliated global network to combat money laundering and terrorist financing.

**Financial intelligence unit (FIU)**

A central national agency responsible for receiving, analyzing and transmitting disclosures on suspicious transactions to appropriate authorities.

**Forfeiture**

The involuntary loss of property or assets as a result of legal action. Generally, the owner of the property that has failed to comply with the law or the property is linked to some sort of criminal activity.

**Freeze**

To prevent or restrict the exchange, withdrawal, liquidation or use of assets or bank accounts. Unlike forfeiture, frozen property, equipment, funds or other assets remain the property of the natural or legal people that held an interest in them at the time of the freezing and may continue to be administered by third parties. The courts may decide to implement a freeze as a means to protect against flight.

**Front company**

Any business set up and controlled by another organization. Although not necessarily illicit, criminals use front companies to launder money by giving the funds the appearance of legitimate origin. Front companies may subsidize products and services at levels well below market rates or even below manufacturing costs.

---

# G

---

**GAFISUD (Spanish: Grupo de Acción Financiera de Sudamérica)**

*See Financial Action Task Force on Money Laundering in Latin America.*

**Gatekeepers**

Professionals, such as lawyers, notaries, accountants, investment advisors and trust and company service providers, who assist in transactions involving the movement of money and are deemed to have a particular role in identifying, preventing and reporting money laundering. Some countries impose due diligence requirements on gatekeepers that are similar to those of financial institutions.

**Grantor**

The party who transfers title or ownership of property or assets. In a trust, typically the person who creates or funds the trust.

**Gulf Cooperation Council (GCC)**

Formed in 1981, the GCC promotes cooperation between its member states in the fields of economy and industry. Member states include Kuwait, Bahrain, Qatar, Saudi Arabia, Oman and the United Arab Emirates. The GCC is a member of FATF, although its individual members are not.

# H

---

**Hawala**

An informal value transfer system common in the Middle East, North Africa and the Indian subcontinent. The system operates outside traditional banking systems. In a basic form, a customer contacts a hawaladar and gives him or her money to be transferred to another person. The hawaladar contacts his or her counterpart where the second person lives, who remits the funds to that person. A running tally is kept between the hawaladars of which owes the other a net sum. *See alternative remittance system.*

**Hawaladar**

A hawala broker.

**Human smuggling**

Human smuggling refers to the transport or illegal entry of a person across international borders in contravention of one or more countries' laws. Human smuggling differs from human trafficking in that it focuses on the entry or transport, rather than the exploitation, of the person involved.

**Human trafficking**

Also known as Trafficking in Persons. The trade of humans, most commonly for the purpose of sexual slavery, forced labor or commercial sexual exploitation. Trafficking occurs in almost every country in the world and is often cited as the second-largest criminal enterprise in the world.

# I

---

**Informal value transfer system (IVTS)**

*See alternative remittance system.*

**Integration**

The integration phase, often referred to as the third and last stage of the classic money laundering process, places laundered funds back into the economy by re-entering the funds into the financial system and giving them the appearance of legitimacy.

**International business company (IBC)**

A variety of offshore corporate structures that are dedicated to business use outside the incorporating jurisdiction and feature rapid formation, secrecy, broad powers, low cost, low-to-zero taxation and minimal filing and reporting requirements.

**International Monetary Fund (IMF)**

An organization of more than 180 member countries, the IMF works to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth and reduce poverty around the world. The organization's objectives have remained unchanged since it was established. Its operations, which involve surveillance, financial assistance and technical support, have adjusted to meet the changing needs of member countries.

**Informal value transfer system (IVTS)**

*See alternative remittance system.*

# K

**Knowledge**

Mental state accompanying a prohibited act. The Interpretive Notes to Recommendation 3 of the FATF 40 Recommendations of 2012 say that countries should ensure that the intent and knowledge required to prove the offense of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such a mental state may be inferred from objective factual circumstances. The exact definition of knowledge that accompanies an anti-money laundering act varies by country. Knowledge can be deemed, under certain circumstances, to include willful blindness; that is “the deliberate avoidance of knowledge of the facts,” as some courts have defined the term.

**Know your customer (KYC)**

Anti-money laundering policies and procedures used to determine the true identity of a customer and the type of activity that is normal and expected, and to detect activity that is unusual for a particular customer.

**Know your employee (KYE)**

Anti-money laundering policies and procedures for acquiring a better knowledge and understanding of the employees of an institution for the purpose of detecting conflicts of interests, money laundering, past criminal activity and suspicious activity.

**Layering**

The second phase of the classic three-step money laundering process between placement and integration, layering involves distancing illegal proceeds from their source by creating complex levels of financial transactions designed to disguise the audit trail and to provide anonymity.

**Legal risk**

Defined by the 2001 Basel Customer Due Diligence for Banks paper as the possibility that lawsuits, adverse judgments or contracts that cannot be enforced may disrupt or harm a financial institution. In addition, banks can suffer administrative or criminal penalties imposed by the government. A court case involving a bank may have graver implications for the institution than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not practice due diligence in identifying customers and understanding and managing their exposure to money laundering.

**Letter of credit**

A credit instrument issued by a bank that guarantees payments on behalf of its customer to a third party when certain conditions are met.

**Letter rogatory**

*See commission rogatoire.*

# M

---

**Memorandum of understanding (MOU)**

Agreement between two parties establishing a set of principles that govern their relationship on a particular matter. An MOU is often used by countries to govern their sharing of assets in international asset-forfeiture cases or to set out their respective duties in anti-money laundering initiatives. Financial intelligence units (FIUs), with the task of receiving and analyzing suspicious transaction reports on an ongoing basis and maintaining close links with police and customs authorities, share information among themselves informally in the context of investigations, usually on the basis of an MOU.

**Middle East and North Africa Financial Action Task Force (MENAFATF)**

A FATF-style body established for the Middle Eastern and North African regions in 2004.

**Monetary instruments**

Traveler's checks, negotiable instruments, including personal checks and business checks, official bank checks, cashier's checks, promissory notes, money orders, securities or stocks in bearer form. Monetary instruments are normally included, along with currency, in the anti-money laundering regulations of most countries, and financial institutions must file reports and maintain records of customer activities involving them.

**Money laundering**

The process of concealing or disguising the existence, source, movement, destination or illegal application of illicitly derived property or funds to make them appear legitimate. It usually involves a three-part system: placement of funds into a financial system, layering of transactions to disguise the source, ownership and location of the funds and integration of the funds into society in the form of holdings that appear legitimate. The definition of money laundering varies in each country where it is recognized as a crime.

**Money laundering reporting officer (MLRO)**

A term used in various international rules to refer to the person responsible for overseeing a firm's anti-money laundering activities and program and for filing reports of suspicious transactions with the national FIU. The MLRO is the key person in the implementation of anti-money laundering strategies and policies.

**Money order**

A monetary instrument usually purchased with cash in small (generally under 500 euros) denominations. It is commonly used by people without checking accounts to pay bills or to pay for purchases in which the vendor will not accept a personal check. Money orders may be used for laundering because they represent an instrument drawn on the issuing institution rather than on an individual's account.

**Money services business (MSB)**

A person (whether a natural or legal person) engaged in any of the following activities where it exceeds the applicable regulatory threshold, at which point the person is generally deemed to be a financial institution subject to AML obligations.

- Dealing in foreign exchange
- Check cashing
- Issuing or selling traveler's checks or money orders
- Providing or selling prepaid access
- Money transmission

**Money transfer service or value transfer service**

Financial service that accepts cash, checks and other monetary instruments that can store value in one location and pay a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third-party final payment. A money or value transfer service may be provided by people (natural or legal) formally through the regulated financial system (e.g., bank accounts), informally through nonbank financial institutions and business entities or outside of the regulated system. In some jurisdictions, informal systems are referred to as alternative remittance services or underground (or parallel) banking systems.

**MONEYVAL**

Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures. Formerly PC-R-EV, the committee was established in 1997 by the Committee of Ministers of the Council of Europe to conduct self and mutual assessments of anti-money laundering measures in place in Council of Europe countries that are not FATF members. MONEYVAL is a sub-committee of the European Committee on Crime Problems of the Council of Europe (CDPC).

**Monitoring**

An element of an institution's anti-money laundering program in which customer activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed normal and expected for the customer.

**Mutual legal assistance treaty (MLAT)**

Agreement among countries allowing for mutual assistance in legal proceedings and access to documents and witnesses and other legal and judicial resources in the respective countries, in private and public sectors, for use in official investigations and prosecutions.

# N

---

**Nesting**

The practice where a respondent bank provides downstream correspondent services to other financial institutions and processes these transactions through its own correspondent account. The correspondent bank is thus processing transactions for financial institutions on which it has not conducted due diligence. Although this is a normal part of correspondent banking, it requires the correspondent bank to conduct enhanced due diligence on its respondent's AML program to adequately mitigate the risk of processing the customer's customers' transactions.

**Nongovernmental organization (NGO)**

Nonprofit organizations that are not directly linked to the governments of specific countries, and perform a variety of service and humanitarian functions, including bringing citizen concerns to governments, advocating for causes and encouraging political participation. Some countries' anti-money laundering regulations for NGOs still have loopholes that some worry could be exploited by terrorists or terrorist sympathizers trying to secretly move money.

**Nonprofit organizations (NPO)**

These can take on a variety of forms, depending on the jurisdiction and legal system, including associations, foundations, fund-raising committees, community service organizations, corporations of public interest, limited companies and public benevolent institutions. FATF has suggested practices to help authorities protect organizations that raise or disburse funds for charitable, religious, cultural, educational, social or fraternal purposes from being misused or exploited by financiers of terrorism.

---

# O

---

**Offshore**

Literally, away from one's own home country—if one lives in Europe, the United States is offshore. In the money laundering lexicon, the term refers to jurisdictions deemed favorable to foreign investments because of low or no taxation or strict bank secrecy regulations.

**Offshore banking license**

A license that prohibits a bank from doing business with local citizens or in local currency as a condition of its license.

**Offshore financial center (OFC)**

Institutions that cater to or otherwise encourage banks, trading companies and other corporate or legal entities to physically or legally exist in a jurisdiction but limit their operations to offshore, meaning outside the jurisdiction (*see offshore*). OFCs have historically been located in the Caribbean or on Mediterranean islands to be in reasonable proximity to the major financial centers of the U.S. and Europe.

**Omnibus account**

*See clearing account.*

**Operational risk**

The risk of direct or indirect loss of operations due to inadequate or failed internal processes, people or systems, or as a result of external events. Public perception that a bank is not able to manage its operational risk effectively can disrupt or harm the business of the bank.

**Organization for Economic Cooperation and Development (OECD)**

International organization that assists governments on economic development issues in the global economy. OECD houses the FATF Secretariat in Paris.

**CICAD (Comisión Interamericana para el Control del Abuso de Drogas or Inter-American Drug Abuse Control Commission)**

CICAD has issued several sets of anti-money laundering recommendations, including amendments to the Organization of American States (OAS) Model Regulations issued in 1992.

**Originator**

The account holder or, where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

# P

---

**Payable through account**

Transaction account opened at a depository institution by a foreign financial institution through which the foreign institution's customers engage, either directly or through subaccounts, in banking activities and transactions in such a manner that the financial institution's customers have direct control over the funds in the account. These accounts pose risks to the depository institutions that hold them because it can be difficult to conduct due diligence on foreign institution customers who are ultimately using the PTA accounts.

**Physical presence**

Existence of an actual brick-and-mortar location with meaningful management of the institution physically located within a country, where it maintains business records and is subject to supervision. The mere existence of a local agent or low level staff does not constitute physical presence.

**Placement**

The first phase of the money laundering process: The physical disposal of proceeds derived from illegal activity.

**Politically exposed person (PEP)**

According to FATF's revised 40 Recommendations of 2012, a PEP is an individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation or important political party official, as well as their families and close associates. The term PEP does not extend to middle-ranking individuals in the specified categories. Various country regulations will define the term PEP, which may include domestic as well as foreign persons.

**Ponzi scheme**

A money laundering system named after Charles Ponzi, an Italian immigrant who spent 10 years in jail in the U.S. for a scheme that defrauded 40,000 people out of \$15 million. Ponzi's name became synonymous with the use of new investors' money to pay off prior investors. Ponzi schemes involve fake, nonexistent investment schemes in which the investors are tricked into investing on the promise of unusually attractive returns. The operator of the scheme can keep the operation going by paying off early investors with the money from new investors until the scheme collapses under its own weight and/or the promoter vanishes with the remaining money.

**Predicate crimes**

Specified unlawful activities whose proceeds, if involved in the subject transaction, can give rise to prosecution for money laundering. Most anti-money laundering laws contain a wide definition or listing of such underlying crimes. Predicate crimes are sometimes defined as felonies or “all offenses in the criminal code.”

**Private banking**

A department in a financial institution that provides high-end services to wealthy individuals. Private banking transactions tend to be marked with confidentiality, complex beneficial ownership arrangements, offshore investment vehicles, tax shelters and credit extension services.

**Private investment company (PIC)**

Also known as a personal investment company, a PIC is a type of corporation that is often established in an offshore jurisdiction with tight secrecy laws to protect the privacy of its owners. In some jurisdictions, an international business company or exempt company is referred to as a private investment company.

**Pyramid scheme**

*See Ponzi scheme.*

# R

---

**Red flag**

A warning signal that should bring attention to a potentially suspicious situation, transaction or activity.

**Regulatory agency**

A government entity responsible for supervising and overseeing one or more categories of financial institutions. The agency generally has authority to issue regulations, to conduct examinations, to impose fines and penalties, to curtail activities and, sometimes, to terminate charters of institutions under its jurisdiction. Most financial regulatory agencies play a major role in preventing and detecting money laundering and other financial crimes. Most regulators focus on domestic institutions, but some have the ability to regulate foreign branches and operations of institutions.

**Remittance services**

Also referred to as giro houses or casas de cambio, remittance services are businesses that receive cash or other funds that they transfer through the banking system to another account. The account is held by an associated company in a foreign jurisdiction where the money is made available to the ultimate recipient.

**Reputational risk**

The potential that adverse publicity regarding a financial institution's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks and other financial institutions are especially vulnerable to reputational risk because they can become a vehicle for, or a victim of, illegal activities perpetrated by customers. Such institutions may protect themselves through know-your-customer and know-your-employee programs.

**Respondent bank**

A bank for which another financial institution establishes, maintains, administers or manages a correspondent account.

**Risk-based approach**

The assessment of the varying risks associated with different types of businesses, clients, accounts and transactions in order to maximize the effectiveness of an anti-money laundering program.

# S

---

**Safe harbor**

Legal protection for financial institutions, their directors, officers and employees from criminal and civil liability for breach of any restriction on disclosing information imposed by contract or by any legislative, regulatory or administrative prohibition, if they report their suspicions in good faith to the financial investigation unit (FIU), even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

**Seize**

To prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freeze, a seizure allows the competent authority to take control of specified funds or other assets. The seized assets remain the property of the individual(s) or entity(ies) that held an interest in them at the time of the seizure, although the competent authority will often take over possession, administration or management of the seized assets.

**Senior foreign political figure**

U.S. term for foreign politically exposed persons. *See politically exposed persons.*

**Settlers**

People or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trust's assets, the deed may be accompanied by a nonlegally binding letter setting out what the settlor wishes done with the assets.

**Shell bank**

Bank that exists on paper only and that has no physical presence in the country where it is incorporated or licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

**Smurfing**

A commonly used money laundering method, smurfing involves the use of multiple individuals and/or multiple transactions for making cash deposits, buying monetary instruments or bank drafts in amounts under the reporting threshold. The individuals hired to conduct the transactions are referred to as smurfs. *See structuring.*

**Sting operation**

Investigative tactic in which undercover officers pose as criminals, sometimes through a front business, to win the confidence of suspected or known criminals to gather information and to obtain evidence of criminal conduct. It is an effective means of identifying criminals, penetrating criminal organizations and identifying tainted property in money laundering and other cases.

**Structuring**

Illegal act of splitting cash deposits or withdrawals into smaller amounts, or purchasing monetary instruments, to stay under a currency reporting threshold. The practice might involve dividing a sum of money into lesser quantities and making two or more deposits or withdrawals that add up to the original amount. Money launderers use structuring to avoid triggering a filing by a financial institution. The technique is common in jurisdictions that have compulsory currency reporting requirements. *See smurfing.*

**Subpoena**

Compulsory legal process issued by a court to compel the appearance of a witness at a judicial proceeding, sometimes requiring the witness to bring specified documents. The term can refer to either the process or the actual document that compels the recipient to act.

**Suspicious activity**

Irregular or questionable customer behavior or activity that may be related to a money laundering or other criminal offense, or to the financing of a terrorist activity. May also refer to a transaction that is inconsistent with a customer's known legitimate business, personal activities or the normal level of activity for that kind of business or account.

**Suspicious activity report (SAR)**

*See suspicious transaction report.*

**Suspicious transaction report (STR)**

A government filing required by reporting entities that includes a financial institution's account of a questionable transaction. Many jurisdictions require financial institutions to report suspicious transactions to relevant government authorities such as its FIU on a suspicious transaction report (STR), also known as a suspicious activity report or SAR.

---

# T

---

**Tax haven**

Countries that offer special tax incentives or tax avoidance to foreign investors and depositors.

**Terrorist financing**

The process by which terrorists fund their operations in order to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves financial support from countries, organizations or individuals. The other involves a wide variety of revenue-generating activities, some illicit, including smuggling and credit card fraud.

**Testimony**

Witness' oral presentation, usually under oath, that describes facts known to the witness.

**Tipping off**

Improper or illegal act of notifying a suspect that he or she is the subject of a suspicious transaction report or is otherwise being investigated or pursued by the authorities.

**Trade finance**

*See letter of credit.*

**Transparency International (TI)**

Berlin-based, nongovernmental organization dedicated to increasing government accountability and curbing both international and national corruption. Established in 1993, TI is active in approximately 100 countries. It publishes corruption news on its website daily and offers an archive of corruption-related news articles and reports. Its Corruption Online Research and Information System, or CORIS, is perhaps the most comprehensive worldwide database on corruption. TI is best known for its annual Corruption Perceptions Index (CPI), which ranks countries by perceived levels of corruption among public officials; its Bribe Payers Index (BPI) ranks the leading exporting countries according to their propensity to bribe. TI's annual Global Corruption Report combines the CPI and the BPI and ranks each country by its overall level of corruption. The lists help financial institutions determine the risk associated with a particular jurisdiction.

**Trust**

Arrangement among the property owner (the grantor), a beneficiary and a manager of the property (the trustee), whereby the trustee manages the property for the benefit of the beneficiary in accordance with terms set by the grantor.

**Trustee**

May be a paid professional or company or unpaid person that holds the assets in a trust fund separate from the trustee's own assets. The trustee invests and disposes of the assets in accordance with the settlor's trust deed, taking into consideration any letter of wishes.

**Typology**

Refers to a money laundering method and is a term used by FATF.

# U

---

**Ultimate beneficial owner (UBO)**

*See beneficial owner.*

**Underground banking**

*See alternative remittance system.*

**United Nations (U.N.)**

An international organization that was established in 1945 by 51 countries committed to preserving peace through cooperation and collective security. Today, nearly every nation in the world belongs to the U.N. *See also Vienna Convention.* The United Nations contributes to the fight against organized crime with initiatives such as the Global Program against Money Laundering (GPML), the key instrument of the U.N. Office of Drug Control and Crime Prevention in this task. Through the GPML, the U.N. helps member states to introduce legislation against money laundering and to develop mechanisms to combat this crime. The program encourages anti-money laundering policy development, monitors and analyzes the problems and responses, raises public awareness about money laundering and acts as a coordinator of joint anti-money laundering initiatives with other international organizations.

**U.N. Security Council Resolution 1373 (2001)**

Adopted in 2001, the resolution requires member nations to take a series of actions to combat terrorism through the adoption of laws and regulations and the establishment of administrative structures. The resolution also requires member nations to “afford one another the greatest measure of assistance for criminal investigations or criminal proceedings relating to the financing or support of terrorist acts.”

**Unusual transaction**

Transaction that appears designed to circumvent reporting requirements, is inconsistent with the account’s transaction patterns or deviates from the activity expected for that type of account.

**USA PATRIOT Act**

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law 107-56). Enacted on October 26, 2001, the historic U.S. law brought about momentous changes in the anti-money laundering field, including more than 50 amendments to the Bank Secrecy Act. Title III of the Act, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, contains most, but not all, of its anti-money laundering-related provisions.

**Value transfer service**

*See money transfer service.*

**Vienna Convention**

Convention in 1988 against the Illicit Trade in Narcotic Drugs and Psychotropic Substances. Countries that become parties to the Vienna Convention commit to criminalizing drug trafficking and associated money laundering, and enacting measures for the confiscation of the proceeds of drug trafficking. Article III of the Convention provides a comprehensive definition of money laundering, which has been the basis of much subsequent national legislation.

**Virtual currency**

A medium of exchange that operates in the digital space that can typically be converted into either a fiat (e.g., government-issued currency) or it can be a substitute for real currency.

# W

---

**Willful blindness**

Legal principle that operates in money laundering cases in the U.S. and is defined by courts as the “deliberate avoidance of knowledge of the facts” or “purposeful indifference.” Courts have held that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.

**Wire transfer**

Electronic transmission of funds among financial institutions on behalf of themselves or their customers. Wire transfers are financial vehicles covered by the regulatory requirements of many countries in the anti-money laundering effort.

**Wolfsberg Group**

Named after the castle in Switzerland where its first working session was held, the Wolfsberg Group is an association of global financial institutions, including Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank and UBS. In 2000, along with Transparency International and experts worldwide, the institutions developed global anti-money laundering guidelines for international private banks. Since then, it has issued several other guidelines on correspondent banking and terrorist financing, among others.

**World Bank**

The World Bank is a vital source of financial and technical assistance to developing countries. It is not a bank in the usual sense, but is made up of two unique development institutions owned by 184 member countries—the International Bank for Reconstruction and Development (IBRD) and the International Development Association (IDA). Both organizations provide low-interest loans, interest-free credit and grants to developing countries. In 2002, the IMF and the World Bank launched a 12-month pilot program to assess countries' anti-money laundering and counter-terrorist financing measures. The World Bank and the IMF, in conjunction with FATF, developed a common methodology to conduct such assessments based on the FATF's 40 Recommendations.

**NOTES:**

[illegible]

[illegible]

[illegible]

# Chapter 6

## Practice Questions

Disclaimer: The practice questions contained within this chapter are not meant to indicate the length or composition of the actual CAMS Examination questions. They are designed to help candidates review the content of the examination manual.

1. Which of the following is the most common method of laundering money through a legal money services business?
  - A. Exchanging currency and remitting money
  - B. Smuggling bulk cash
  - C. Transferring funds through payable through accounts (PTAs)
  - D. Exchanging Colombian pesos on the black market
2. In general, the three phases of money laundering are said to be: placement and
  - A. structuring and manipulation.
  - B. layering and integration.
  - C. layering and smurfing.
  - D. integration and infiltration.
3. Which statement is true?
  - A. Systemic weaknesses in free trade zones include inadequate AML/CFT safeguards, minimal oversight by local authorities and weak procedures to inspect goods.
  - B. Cuckoo smurfing is a significant money laundering technique identified by the Financial Action Task Force, wherein a form of structuring uses nested accounts with shell banks in secrecy havens.
  - C. In its 40 Recommendations, the FATF issued a list of designated categories of offense that asserts crimes for a money laundering prosecution.
  - D. E-cash is not attractive to the money launderer because it cannot be completely anonymous and does not allow for large amounts to be transported quickly and easily.

4. Which three of the following is an indication of possible money laundering in an insurance industry scenario?
  - A. Insurance products sold through intermediaries, agents or brokers
  - B. Single-premium insurance bonds, redeemed at a discount
  - C. Policyholders who are unconcerned about penalties for early cancellation
  - D. Policyholders who redeem the policy within the free look period
  
5. Which two activities are typically associated with the black market peso exchange (BMPE) money laundering system?
  - A. Converting illicit drug proceeds from dollars or euros to Colombian pesos
  - B. Converting illicit drug proceeds from Colombian pesos to dollars or euros
  - C. Facilitating purchases by Colombian importers of goods manufactured in the United States or Europe through peso brokers
  - D. Facilitating purchases by European or U.S. importers of goods manufactured in Colombia through peso brokers
  
6. What is the right of reciprocity in the field of international cooperation against money laundering?
  - A. The legal principle that financial institutions that have referred customers to other financial institutions can share information about these customers with the other institutions
  - B. A rule of the Basel Committee allowing properly regulated financial institutes of another member state of the Basel Committee to do business without additional supervision to the degree that the other state grants the same right
  - C. The right of each FATF member country to delegate prosecution of a case of money laundering to another member that is already investigating the same case
  - D. A rule in the law of a country allowing its authorities to cooperate with authorities of other countries to the degree that their law allows them to do the same
  
7. The greatest risk for money laundering is for casinos that
  - A. provide their customers with a wide array of gambling services.
  - B. operate in a non-Egmont member country.
  - C. allow customers with credit balances to withdraw funds by check in another jurisdiction.
  - D. only send suspicious transaction reports to the financial intelligence unit of the country it operates in.

8. Which statement is true regarding the risk of politically exposed persons (PEPs)?
- A. PEPs provide access to third parties on whom the financial institution has not conducted sufficient due diligence.
  - B. PEPs have significantly greater exposure to the politically corrupt funds, including accepting bribes or misappropriating government funds.
  - C. PEPs are foreign customers who inherently present additional risk as they are engaged in cross-border transactions.
  - D. PEPs generally do not pose enhanced risks to an institution due to their political standing; rather, PEPs increase the prestige of an institution.
9. In 2014, the Wolfsberg Group published its Anti-Money Laundering Principles for Correspondent Banking. Which three of the following elements are recommended to be included in the due diligence of a correspondent banking client?
- A. The geographic risk
  - B. The ownership and management structure
  - C. The résumé of the compliance officer
  - D. The customer base
10. A new customer approaches a bank to open a commercial account. The customer provides an address for the account located across the city from the branch. When asked by the account representative if the customer requires any additional banking services, the customer responds that she is also interested in opening a personal investment account. The account representative refers the customer to the broker-dealer. The customer tells the firm representative she has never had a brokerage account before and has a few questions about how an investment account works. The customer asks how deposits can be made into her account, if there are any reporting requirements, and how to go about moving balances out of the account using wire transfers. No questions are asked about fees associated with these transactions. Which three items would be considered suspicious?
- A. The customer asks many questions about the brokerage account but none of them is related to investing.
  - B. The customer is opening a commercial account and at the same time a personal investment account.
  - C. The address of the account holder and the branch where the customer came to open the account are not close to each other.
  - D. The customer appears unconcerned about the fees.

11. Trade-based money laundering requires the ability to
- A. over- or under-invoice the goods.
  - B. sell the imported goods for as little as possible.
  - C. use goods that do not need to be declared.
  - D. avoid the use of high-value assets such as luxury cars or boats.
12. Which of the following statements is true? Correspondent banking is *most* vulnerable to money laundering when the correspondent account is
- A. maintained for foreign financial institutions that are banks.
  - B. not used to provide services directly to third parties.
  - C. maintained for a foreign bank that does not have a physical presence in any country.
  - D. maintained for a foreign private bank that is publicly traded and is a qualified intermediary.
13. Which statement is true?
- A. Lawyers in FATF member countries generally cannot be used to serve as formation agents to set up trusts, front companies or shell companies.
  - B. Lawyers and similar professional gatekeepers are called money services businesses.
  - C. Lawyers generally cannot be used to act as nominee shareholders for a beneficial owner.
  - D. Lawyers can be abused by launderers by using the accounts they set up for them for the placement and layering of funds.
14. Which three of the following statements are true in respect to the Fourth EU Anti-Money Laundering Directive?
- A. Member countries can decide when and if they incorporate it into their local laws.
  - B. It repeals and replaces the Third EU Directive on Anti-Money Laundering.
  - C. Each member country must hold beneficial ownership information in a central registry and it must be made available to competent authorities.
  - D. The definition of a PEP is expanded to include domestic persons.

15. According to the EU Directives, an independent legal professional is obligated to report suspicion of money laundering in a client relationship when
- A. representing a client in a legal matter.
  - B. ascertaining the legal position for a client.
  - C. participating in financial or corporate transactions.
  - D. obtaining information associated with a judicial proceeding.
16. Which of the following is the most difficult regulatory challenge facing a foreign financial institution with a correspondent banking relationship in the U.S.?
- A. USA PATRIOT Act
  - B. Basel Due Diligence Principles for Banks
  - C. FATF Guidance on Terrorist Financing
  - D. UN Security Council Resolution on Correspondent Banking
17. Which were the Basel Committee's two main motivations to encourage strong know your customer programs in its paper *Customer Due Diligence for Banks*? (Choose two)
- A. Mirror FATF's KYC recommendations.
  - B. Meet European Union guidelines.
  - C. Protect the safety and soundness of banks.
  - D. Protect the integrity of banking systems.
18. What is the definition of a predicate offense?
- A. Lawful or unlawful activity that involves willful blindness, and if there is an international element to the crime, can lead to a suspicious activity report
  - B. Unlawful activity whose proceeds, if involved in the transaction, can give rise to prosecution for the crime of money laundering
  - C. An interface that is the underlying segment of a suspicious transaction monitoring system
  - D. A specified unlawful activity that is committed through concentration accounts deceiving customers that are not directly related to the account

19. What is considered a beneficial owner of an account?
- A. A person or entity who has direct signatory authority over an account and whose name appears on the account
  - B. A person or entity who is ultimately entitled to the funds in the account, even though his or her name may not appear on the account
  - C. A person or entity who is the originator and the destination of most (but not all) transactions conducted within the account but who does not ultimately control such funds
  - D. A person or entity who is a gatekeeper, has the legal title to the account and typically transfers the funds to a trust
20. FinCEN's *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance*, published in 2014, listed six areas of emphasis. Which three areas are included in that list?
- A. Leadership should be engaged.
  - B. Information should be shared throughout the organization.
  - C. Leadership and staff should understand how their BSA reports are used.
  - D. The organization must have an appropriately qualified compliance officer.
21. Which of the following should a national legislature consider when criminalizing money laundering in line with the CFATF 19 Recommendations? (Choose three.)
- A. Defining money laundering based on the model laws issued by the Organization of American States
  - B. Permitting forfeiture in all cases following conviction
  - C. Indicating whether it is relevant that a predicate offense may have been committed outside the local jurisdiction
  - D. Requiring money laundering offenses to prove that the offender has actual knowledge of a criminal connection to the funds
22. Which three statements are true about the Fourth EU Directive on Money Laundering?
- A. It updates European Community legislation to be further in line with the Financial Action Task Force (FATF) 40 Recommendations.
  - B. It repeats the definition of a politically exposed person in previous directives.
  - C. It repeats the customer due diligence requirements of the previous directives but adds more detail to the requirements by, for example, including a specific requirement to identify the beneficial owner and includes ongoing monitoring requirements.
  - D. It includes new definitions for correspondent relationships and senior management.

23. Which one of the following statements is correct in respect of the FATF 40 Recommendations? Countries should
- A. not allow bearer shares and legal persons that are able to issue bearer shares.
  - B. gather statistics on STRs; prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance, but not necessarily on other international requests for cooperation.
  - C. consider the feasibility of a system in which banks and other financial institutions and intermediaries would report currency transactions without indicating a minimum fixed amount.
  - D. not approve the establishment or accept the continued operation of shell banks.
24. The Egmont Training Group published *FIUs in Action: 100 Sanitized Cases*. Which two of the items noted below were listed in the report as part of the six most frequent indicators of money laundering?
- A. Defensive stance to questioning
  - B. Use of precious stones for moving value
  - C. Unrealistic wealth compared to client profile
  - D. Significant use of prepaid cards
25. In which stage of money laundering would you classify depositing small amounts of cash into several related accounts?
- A. Integration
  - B. Structuring
  - C. Placement
  - D. Construction
26. In which stage of money laundering would you classify the use of laundered funds to purchase high-value assets and luxury items?
- A. Integration
  - B. Structuring
  - C. Placement
  - D. Construction

27. In most money laundering international standards, it is stated that
- A. financial institutions are not responsible for money laundering or suspicious transactions taking place within their accounts until the government places the customer on a watch list.
  - B. informing customers that their accounts and/or transactions are the subject of an AML investigation is not punishable.
  - C. the dirty money undergoing money laundering will not be confiscated because of privacy laws.
  - D. the institution should identify the beneficial owner(s) of the account.
28. The tactic in which individuals make multiple deposits in small quantities to avoid detection is called
- A. paralleling.
  - B. integration.
  - C. investing.
  - D. structuring.
29. In which case might a suspicious transaction report *not* be necessary?
- A. A customer deposits money of suspicious origins and refuses to answer questions from the financial institution's staff.
  - B. A customer tries to move money that is suspected of being derived from criminal activity.
  - C. A customer owns a large supermarket and deposits large amounts of cash several times a day.
  - D. A customer's account is showing transaction activities that are beyond his known financial capability.
30. As part of their role in fighting money laundering, financial institutions should
- A. designate a compliance officer.
  - B. depend solely on the state's staff for combating money laundering.
  - C. refuse small cash deposits under the reporting threshold.
  - D. not open accounts for people from high-risk jurisdictions.

31. Over lunch with a friend from the computer operations department, a junior compliance analyst learns that there was a problem during the previous week related to data being transmitted to the transaction monitoring application. The friend states that because it was purely a technical computer system issue, he was quietly proud that he was able to rectify it quickly himself during the early hours of the morning. What action should the analyst take?
- A. Congratulate his friend on his prompt action.
  - B. Congratulate his friend and, as soon as possible, ensure that the compliance officer is aware of the situation.
  - C. Nothing because the appropriate controls are in place for such events.
  - D. Immediately report the situation to the regulators.
32. What is willful blindness defined as?
- A. Failing to file a suspicious transaction report for dealing with companies or financial institutions from offshore tax havens
  - B. Not following customer identification procedures as set out in the institution's procedures
  - C. Deliberate avoidance of knowledge of the facts or ignoring obvious money laundering red flags
  - D. Deliberate avoidance of a customer based on the assumption that his or her behavior suggested a potential threat as money launderer and/or terrorist
33. In anti-money laundering terminology, a red flag is
- A. a warning sign indicating potentially suspicious, risky transactions or activities.
  - B. a general banking term used once the balance is negative or overdue.
  - C. the standard flag of countries not cooperative in fighting money laundering and terrorist financing.
  - D. an indicator that a customer is listed on an economic sanctions list.
34. The money laundering reporting officer of a financial institution should
- A. report everything that comes his or her way from anyone in the organization.
  - B. report everything that comes his or her way from senior management or Board of Directors.
  - C. review all available information and file a suspicious transaction report in respect of any unusual or potentially suspicious activity.
  - D. report only what the reporting officer's superior agrees should be reported.

35. Which of the following statements is true?
- A. Credit cards are not likely to be used in the layering phase of money laundering because of restrictions in cash payments.
  - B. Credit cards are effective instruments for laundering money because the transactions do not create an audit trail.
  - C. A launderer can launder money by prepaying his or her credit card using funds that are already in the banking system, creating a credit balance on his account, and requesting a credit refund.
  - D. A launderer can use illicit funds that are already in the banking system to pay his or her credit card bill for goods purchased, which is an example of placement.
36. Why is a payable through account vulnerable to money laundering?
- A. It can be very difficult to conduct due diligence on the foreign institution customers who are ultimately using these accounts.
  - B. These are concentration accounts located in a domestic branch of a foreign bank.
  - C. These are nested correspondent accounts at a foreign shell bank with customers with whom the domestic bank did not exercise due diligence.
  - D. These are master escrow accounts on which a domestic bank generally does not conduct periodic verification.
37. What is the reasoning behind implementing a risk-based anti-money laundering approach?
- A. It will keep the regulators focused on money laundering controls in sectors beyond banks.
  - B. Institutions can best use their limited resources to focus on matters where the money laundering risks are highest.
  - C. A quantitative approach will generate better results than a qualitative approach.
  - D. It allows the institution to focus on selling products that have a better return on investment.
38. According to the FATF 40 Recommendations, designated nonfinancial businesses and professions include
- A. casinos, real estate agents and dealers in precious stones.
  - B. money service businesses, gatekeepers and issuers of electronic money.
  - C. dealers in precious metals, lawyers and commodity futures traders.
  - D. life insurance companies, real estate agents and notaries.

39. In the 4th EU directive, to what level has the threshold decreased for inclusion of natural or legal persons trading in goods and making/receiving cash payments?
- A. \$5,000 euros.
  - B. \$10,000 euros.
  - C. \$15,000 euros.
  - D. \$20,000 euros.
40. Tom works as a compliance officer at ABC Bank. He is looking at the transactions of one of the bank's customers, Mr. Brown, the owner of a check cashing company. Over the last six months, Mr. Brown has not made withdrawals of cash against check deposits. He also deposited two checks for \$2,000 each that were issued by a casino. When checking the KYC file, Tom sees that, when opening the account, Mr. Brown had requested information about fees and commission that are charged by the bank. What should arouse Tom's suspicion the most?
- A. Mr. Brown deposited checks from casinos.
  - B. Mr. Brown has not made cash withdrawals against check deposits.
  - C. Mr. Brown asked for information about commissions and fees charged.
  - D. Mr. Brown does not have an escrow account.
41. A small broker-dealer has an AML compliance program that addresses procedures for filing suspicious transaction reports and includes policies, procedures and internal controls for customer identification, monitoring accounts and identifying money laundering red flags. Every employee of the broker dealer is trained via the Internet in January and in July on AML issues. The board does not take the Internet training. Instead, the compliance officer organizes a luncheon for them where an outsider comes in and trains them. The program provides for the appointment of a compliance officer, and once a year the compliance officer conducts an audit to test the program. In what respect does the program need improvement?
- A. The AML program should be tested by an independent person, not the compliance officer.
  - B. The AML program should be tested more than once per year.
  - C. The board should receive the same training provided to the employees.
  - D. Employees should not be trained via the Internet, because classroom training is better.

42. The Basel Committee in Banking Supervision can be defined as a committee
- A. that develops the guidance for FATF.
  - B. of the CEOs of the major international banks.
  - C. of senior members of international law enforcement who harmonize international AML/CTF laws.
  - D. of the G10 central bank governors, which issues guidance on subjects including customer due diligence, risk management and cross-border wire transfers.
43. Which of the following best describes the alternative remittance system?
- A. The transfer of value between countries, outside of the legitimate banking system
  - B. A nonelectronic data remittance system used in several foreign countries to report suspicious activities
  - C. Old-fashioned reporting requirements commonly used in non-cooperative countries and territories
  - D. The transfer of funds between two or more financial institutions using concentration accounts
44. An AML compliance officer was reviewing customers at XYZ Bank and one of the customers (Mr. Sam Tropicana) attracted her attention. During the recent months, the cash deposits and withdrawals that were transacted through his account increased with amounts ranging between \$7,500 and \$17,000. In addition, Sam deposited two checks, issued by a casino, into his account for \$32,000 each. When opening the account, Sam stated that he operated an import/export company. Which one of the following items should cause the compliance officer to launch an investigation?
- A. Sam maintained a personal account as well as the business account.
  - B. Sam's home telephone number was disconnected last month.
  - C. Sam asked for a letter of credit to finance some imports from a new supplier.
  - D. Sam had a recent increase in large cash transactions for his import/export business.
45. Which three of the following statements are true?
- A. Online gambling provides an excellent method of laundering because transactions are conducted primarily through credit or debit cards and the sites are typically unregulated offshore firms.
  - B. An institution can know when a credit card is used for online gambling transactions because the cards rely on codes that illustrate the type of transactions.
  - C. Online gambling provides an excellent method of laundering because it lends itself to any type of cash movement and there is no face-to-face contact with the customer.
  - D. Some banks no longer allow the use of credit cards for online gambling transactions.

46. Which of the following statements is true?
- A. The Egmont Group membership comprises national FIUs.
  - B. The Wolfsberg Group membership comprises central bank governors of the G10.
  - C. The European Union recommends legislation to be passed in the member countries.
  - D. The Basel Committee levies fines on the member countries for non-compliance with AML laws.
47. Which three of the following statements are included in Section 313 of the PATRIOT Act definition of *physical presence* in respect to shell banks?
- A. There is a fixed address.
  - B. It employs at least one full-time employee.
  - C. The majority of the board of directors must be local residents.
  - D. Banking records are kept at the fixed address.
48. The FATF has consistently noted the use of casinos in money laundering schemes in its annual typologies reports. One laundering technique involving casinos is
- A. asking for winners' checks to be made out in the name of third persons or without a payee.
  - B. abusing casinos by circumventing its gatekeepers.
  - C. prepaying a casino token or chip by using funds that are already in the casino system, creating a debit balance.
  - D. extensive gambling via multiple games throughout the casino.
49. Which of the following should an anti-money laundering specialist include on an internal investigation log?
- A. A government order on a customer that garnishes his wages for failure to pay child support
  - B. Supporting documentation and materials for denying service to a client with a bad credit rating
  - C. Notes pertaining to activity that is unusual but for which a suspicious transaction report has not been filed
  - D. Reference to a memorandum to the company's corporate management relating to budgetary and similar concerns

50. What are the three key criteria in AML risk rating?
- A. Customer type, geographic location, products and services used
  - B. Geographic location, customer type, employment status
  - C. Products and services used, customer type and prior banking relations
  - D. Employment status, customer type, products and services used
51. A financial institution is looking to establish an online account opening service. The institution plans to offer this product to new and existing customers within the country. Which of the following would be the best plan of action for an AML specialist to recommend enabling the institution to verify the customer's identity?
- A. Do not offer the product, because it is too high risk because the customers cannot be seen to verify their identities.
  - B. Require all customers to send a copy of valid photo identification to the institution.
  - C. Ensure that the institution has a reliable third-party source that will enable verification of the customers.
  - D. Allow customers to enter required information but require all customers to come to the institution in person for verification.
52. Which of the following controls would most effectively minimize the need to correct failures to collect required customer information in the account opening process?
- A. A quality review staff that checks paper applications to ensure all fields are complete
  - B. An automated account-opening platform that requires data entry prior to allowing the account to be opened
  - C. Requiring that a manager review and approve all new account applications
  - D. Documenting a procedure that sets forth the steps required to open an account
53. Jane, an investigator in the AML section of a large financial institution, is given a wide-ranging case to investigate involving potential money laundering in a number of countries and entities. Which three public source documents or records could aid Jane in furthering her investigation?
- A. Domestic corporate filings
  - B. Court records
  - C. Police arrest records
  - D. Licensing and registration files

54. When drafting an AML policy, which of the following internal parties must approve the policy?
- A. Executive management
  - B. The audit department
  - C. The sales team management
  - D. The operational staff management
55. Suzy is an AML compliance officer at an institution that is looking to open treasury management services (e.g., wires, check clearing and foreign draft issuance) for correspondent banking customers. Which of the following should Suzy be most concerned about regarding the institution's capabilities concerning these customers?
- A. Whether the new account systems will be able to handle customers with foreign names
  - B. Whether the correspondent accounts will be approved by government regulators
  - C. Whether the correspondent accounts will be able to provide evidence of their customers' identities at account opening
  - D. Whether the correspondent accounts will be able to be monitored by the institution's monitoring systems
56. What are three specific sources of funds for financing terrorism?
- A. Kidnapping for ransom
  - B. Trafficking in humans and arms
  - C. Contributions to charities
  - D. Wiring funds internationally
57. A customer wants to establish a sizable relationship with a financial institution. The AML officer is not comfortable with the client's explanation for the source of the funds, but the client manager vouches for the client and is eager to open the relationship quickly. What should the AML officer do to validate the client's sources of funds?
- A. Accept the client manager's approval of the client.
  - B. Allow the account to be opened but be sure to monitor the account activity.
  - C. Perform a background investigation to determine whether the client's source of funds is credible.
  - D. Decline the account.

58. An AML compliance officer is investigating unusual activity that she has noticed in a customer's accounts. The customer has a retirement account, a savings account in trust for his son, a joint checking account with his wife, a company checking account and an individual brokerage account. The compliance officer believes the customer may be embezzling funds from his business. Which is the best path for her to follow up on her suspicions?
- A. Focus on the checking accounts, as the checking accounts allow the fastest movement of funds.
  - B. Ignore the savings and brokerage accounts, as these are not used in the placement stage of money laundering.
  - C. Look at the movement of funds in all the accounts, as the customer may be using all of them to launder money.
  - D. Focus on the business account, as the customer is embezzling money from the company.
59. Identify three risks to financial institution employees for violations of AML laws.
- A. Civil penalties
  - B. Termination of employment
  - C. Criminal penalties
  - D. Loss of passport
60. A customer at a brokerage firm indicated that he was primarily a conservative, long-range investor. The customer has recently been engaging in day trading in penny stocks. What should an AML compliance officer do in such a situation?
- A. Check with the account officer to see if the customer has indicated a change in his investment strategy.
  - B. Report the customer as suspicious due to investing in penny stocks.
  - C. Contact the customer and ask why he is engaged in high-risk day-trading activity.
  - D. Refer the customer to senior management for approval.

61. A financial institution branch manager who has been in place for over 10 years has not taken a vacation for almost four years. The company does not allow employees to roll vacation over from year to year. An AML compliance officer has noticed unusual activity in several accounts at the branch location. What should the AML officer do?
- A. Fire the manager for violation of bank policy.
  - B. Report the manager to authorities for engaging in suspicious activity.
  - C. Conduct an investigation to establish whether the manager has engaged in transactions in the accounts where the unusual activity has occurred.
  - D. Conduct a background check to see if the manager has been convicted of criminal activity.
62. An AML compliance officer is looking to establish a suspicious activity reporting process at her small institution. Which of the following should be incorporated into the procedures?
- A. Allow employees to refer suspicious activity directly to the government authorities to file as quickly as possible.
  - B. Have employees refer all unusual activity to the internal independent audit department to assess whether the activity should be reported.
  - C. Have employees refer all unusual activity to senior management to ensure they are aware of all unusual activity within the organization.
  - D. Have employees refer all unusual activity to her so that she may conduct an investigation into what needs to be reported to authorities.
63. After reporting suspicious activity to the appropriate authorities, they request additional follow-up on the reports. Which of the following actions should an AML compliance officer take?
- A. Inform the customer that his or her activity has been reported as suspicious and the authorities are asking about him or her.
  - B. Indicate to the authorities that you have fulfilled your regulatory duty by referring the matter to them.
  - C. Give the authorities everything they request.
  - D. Cooperate fully with the authorities, as permitted by law.

64. A compliance officer is looking to improve a compliance program for a financial institution that operates in several countries. The institution has developed consistent customer due diligence (CDD) requirements for all customers of the institution that exceed each of the individual country's requirements. When looking to provide management reporting on the CDD compliance efforts of the institution, which of the following would make the most sense?
- A. Report by each country's compliance with the legal requirements within their country.
  - B. Report on compliance with the company's stated requirements.
  - C. Report on compliance with each country's requirements only for those customers that are serviced by branches in multiple countries; all others should be reported on the company's stated requirements.
  - D. Report on the level of monitoring performed on the activity in the accounts.
65. What is the best way to establish compliance as a key responsibility for every employee of a financial institution?
- A. Have senior management require compliance as a condition of employment.
  - B. Have auditors conduct testing on employee compliance.
  - C. Point out the regulatory consequences of non-compliance in training.
  - D. Have the AML officer personally tell associates of their responsibilities.
66. The *Annex IV General Guide to Account Opening Consultative Document* published in February 2016 by the Basel Committee lists information that should be obtained for the identification of *legal persons*. Which three items are recommended?
- A. Name, legal form, status and proof of incorporation of the legal person
  - B. Permanent address of principal place of the legal person's activities
  - C. A report describing a visit, by the account officer, to the principal place of business
  - D. Identity of natural persons who have authority to operate the account and who exercise control of the legal person through ownership or other means

67. Robert is a compliance officer for a financial institution. He is looking to assess the effectiveness of the current AML program. Which of the following should Robert consider in his assessment of the program's effectiveness?
- A. Sales staff surveys on AML efforts, customer due diligence error rates and quality assurance testing on STR filings
  - B. Customer due diligence error rates, sales staff surveys on AML efforts and percentage of products and services monitored for suspicious activity
  - C. Quality assurance testing on STR filings, sales staff surveys on AML efforts and percentage of products and services monitored for suspicious activity
  - D. Customer due diligence error rates, quality assurance testing on STR filings and percentage of products and services monitored for suspicious activity
68. Joe, the compliance officer for a small bank, has noticed that new regulations now require reporting on cross-border transactions that exceed a certain threshold. What are the appropriate next steps for Joe to take to prepare his bank for the new requirements?
- A. Consult with the regulators, provide training to impacted associates and work with the technology partners to capture all cross-border transactions for reporting.
  - B. Provide training to impacted associates, work with technology partners to capture all cross-border transaction for reporting and implement a testing plan to be sure appropriate transactions are captured and reported.
  - C. Work with technology partners to capture all cross-border transactions for reporting, implement a testing plan to be sure appropriate transactions are captured and consult with the regulators.
  - D. Implement a testing plan to be sure appropriate transactions are captured and reported, provide training to impacted associates and consult with the regulators.
69. When documenting ongoing training efforts, which of the following should be documented to demonstrate the distribution of the training to appropriate employees?
- A. Whether the training was provided to the board of directors
  - B. The topics the training addressed
  - C. The names of the employees who took the training with their department name
  - D. Whether the employees who took the training passed the posttraining assessment

70. When assessing a new product, which of the following should be considered as part of the assessment from an AML perspective?
- A. The inherent risk of the product, the control environment to mitigate the risks presented by the product and the residual risk of the product in light of the controls
  - B. The control environment to mitigate the risks presented by the product, the residual risk of the product in light of the controls and the projected profitability of the product
  - C. The projected profitability of the product, the control environment to mitigate the risks presented by the product and the inherent risk of the product
  - D. The residual risk of the product in light of the controls, the inherent risk of the product and the projected profitability of the product
71. Marie, a compliance officer at a financial institution, attends an annual AML-industry conference and learns of a new regulation that will impact her current AML processes. The regulatory environment has been relatively stable within the industry for several years but Marie is glad she attended this conference to get news of the new requirements. What should Marie do to stay abreast of future changes in requirements?
- A. Request permission to attend future annual AML-industry conferences.
  - B. Ask internal auditors to provide her with notice of changes needed to the program.
  - C. Implement a process to determine when new regulations are published and assess them for impacts to the AML program.
  - D. Conduct a risk assessment to determine if the regulations change frequently enough to implement a process to check for changes.
72. A compliance officer is looking to provide some way to report on the effectiveness of the AML program to senior management. Which of the following would be the most appropriate means to keep senior management informed of these efforts?
- A. Develop a report containing metrics that reflect the effectiveness of various key program elements.
  - B. Rely on the regulatory examinations.
  - C. Provide a summary of all reported suspicious activity.
  - D. Provide detailed training to senior management on their AML obligations.

73. Which statement is true in respect to the Wolfsberg Group?
- A. It is a castle in Belgium where members of national FIUs meet to monitor global AML trends.
  - B. This group is responsible for making international laws to combat anti-money laundering and counter terrorist financing.
  - C. The major international banks meet in this group to develop global guidelines for anti-money laundering and counter terrorist financing.
  - D. The governors of central banks meet in this group to discuss global trends in anti-money laundering and counter terrorist financing.
74. The FATF 40 Recommendations are organized into seven groups. Which three of the following are valid group names?
- A. Money Laundering and Confiscation
  - B. Financial and Non-Financial Institution Preventative Measures
  - C. Powers and Responsibilities of Competent Authorities and Other Instructional Measures
  - D. National Cooperation
75. A longtime customer of the bank comes into the bank a number of times over a series of weeks and deposits a large amount of cash and, the next day, asks for the amount to be wired to a third-world country. This behavior is not in keeping with his normal business practices. What should the compliance officer recommend?
- A. Contact the board of directors as soon as possible and inform them of this activity.
  - B. Immediately contact law enforcement by phone and tell them of the potential money laundering activity.
  - C. Open an internal investigation, collect all the appropriate documentation and review it in order to decide on whether to file an STR.
  - D. Make a note of the activity but do not file an STR to avoid the risk of losing a longtime customer.

76. Which statement below defines a mutual legal assistance treaty?
- A. It is a written request for legal or judicial assistance sent by the central authority of one country to the central authority of another when seeking assistance from the foreign jurisdiction.
  - B. It is an agreement among countries allowing for mutual assistance in legal proceedings and access to documents, witnesses and other legal and judicial resources in the respective countries, in private sectors, for use in official investigations and prosecutions.
  - C. It is an agreement between two parties establishing a set of principles that govern their relationship on a particular matter. An MOU is often used by countries to govern their sharing of assets in international asset-forfeiture cases or to set out their respective duties in anti-money laundering initiatives.
77. After receiving an STR regarding a customer account, the relevant law enforcement agency requests permission to interview the bank personnel who are familiar with the underlying transaction. What action should the compliance officer take?
- A. The officer, in consultation with bank counsel, should cooperate, to the extent possible, and give permission for the relevant interviews to take place.
  - B. The officer should deny permission for any such interviews without the creation of a grand jury or a formal court-ordered investigation.
  - C. The officer should only allow those employees who are comfortable to be interviewed by law enforcement.
  - D. The officer should allow the employees to be interviewed only if they are given immunity by law enforcement.
78. What three factors should a prosecutor take into consideration when deciding whether to bring criminal charges against a financial institution?
- A. Whether the institution has a criminal history
  - B. Whether the institution cooperated with the law enforcement investigation
  - C. Whether the institution discovered and self-reported the potential criminal violation
  - D. Whether the institution is a very large institution and its prosecution will make good headlines for the law enforcement agency

79. The Egmont Group is supported by working groups. Which three are members of the five working groups?
- A. Operational
  - B. Legal
  - C. Examination
  - D. Outreach
80. Gatekeepers are defined as
- A. professionals such as lawyers, accountants, notaries and foreign exchange dealers.
  - B. professionals such as lawyers, accountants, notaries, investment advisors and trust and company service providers.
  - C. professionals such as lawyers, accountants, private bankers, investment advisors and trust and company service providers.
  - D. professionals such as lawyers, accountants, notaries and fraud examiners.
81. The compliance officer is trying to put together a set of procedures for handling the decision of whether or not to file an STR. What should the compliance officer include as part of these procedures?
- A. The officer should recommend that the decision as to whether or not to file an STR be subjected to a quality assurance review.
  - B. The officer should recommend decentralizing the decision in order to speed up the process and to ensure that the decision is made closest to where the activity occurred.
  - C. The officer should recommend that STRs only be filed once they have been authorized by the board of directors of the bank.
  - D. The officer should recommend that STRs only be filed once they have received a thorough legal review.
82. Of the following scenarios, which two are potential red flags indicating possible suspicious activity that should be investigated further?
- A. A large family with multiple accounts held in the name of different family members
  - B. Accounts held for a business in a branch that is located on the other side of town from where the business is located
  - C. An individual who holds multiple accounts under the same name
  - D. A company that has multiple accounts, one for each of their various subsidiary businesses

83. The FATF 40 Recommendations are grouped into seven topics. Identify three of those topics from the list below.
- A. Terrorist Financing and Financing of Proliferation
  - B. Powers and Responsibilities of Competent Authorities and Other Institutional Measures
  - C. Money Laundering and Confiscation
  - D. Financial and Non-Financial Institution Preventative and Detection Measures
84. When would a financial institution typically file an STR?
- A. Whenever it is preparing to close an account
  - B. Whenever it detects unusual or suspicious transactions
  - C. Only when it is able to establish the existence of a criminal violation
  - D. Only when the board of directors approves the filing of the STR
85. When a bank receives a subpoena for information about a specific account, what two steps should the compliance officer take?
- A. The compliance officer should ensure that the staff investigate and collect all documents responsive to the subpoena.
  - B. The compliance officer should insist on law enforcement explaining why the subpoena was issued and what law enforcement is looking for.
  - C. The compliance officer should ensure that the subpoena is reviewed by senior management and/or counsel and be responded to in a timely manner.
  - D. The compliance officer should only comply with the subpoena after first getting approval from the bank's external legal counsel.
86. A law enforcement representative calls up the compliance officer and urgently requests information pertaining to a particular account in connection with an on-going terrorist financing investigation. What should the compliance officer do?
- A. Get permission from the board of directors to hand the material over to law enforcement.
  - B. Hand the material over to law enforcement immediately because of the urgent nature of the request.
  - C. Request that the law enforcement representative provide a court order, a grand jury subpoena or other legal process unless the bank has already filed an STR on the matter.
  - D. Get permission from outside legal counsel before handing the material over to law enforcement.

87. In conducting a criminal investigation, what are three things that the law enforcement investigators should do?
- A. Conduct computer-based searches on the individuals and entities involved.
  - B. Review any previously filed STRs on the individuals and entities involved.
  - C. Analyze the financial transactions and activity of the subject and determine what is potentially illegal.
  - D. Initiate a Section 314(b) request for information.
88. The compliance officer reads about a large potential fraud case in the morning newspaper. When the officer gets to the bank, the officer uncovers the fact that the potential fraud case involves an important customer of the bank. After doing an internal investigation, the officer determines that there is no suspicious activity in the customer's accounts. What should the officer do next?
- A. The officer should notify the board of directors of the nature and results of the internal investigation.
  - B. The officer should document the nature and results of the internal investigation and keep the documentation in an appropriate file.
  - C. The officer should file an STR in case the customer's accounts could assist law enforcement in its formal criminal investigation.
  - D. The officer should file an STR in order to justify the time spent on the internal investigation and to avoid being second-guessed by the bank examiners.
89. What are three developments that should cause a financial institution to conduct an internal investigation?
- A. When the institution receives a grand jury subpoena with regard to transactions that have occurred within several accounts at the institution
  - B. When several employees of the institution alert senior management or the compliance officer that there are some suspicious transactions within an account
  - C. When the institution's auditor identifies an omission in the AML policy
  - D. When a small local business starts engaging in overseas activity involving numerous, unexplained wire transfers

90. What are three possible red flags indicating suspicious or unusual activity that might warrant an investigation and the filing of an STR?
- A. The opening of a new account without a local telephone number or utility bill available
  - B. Unusually high monthly balances in comparison to known sources of income
  - C. High level of monetary transactions through an account during the course of a month but low beginning and ending balances
  - D. Multiple cash deposits made just under the reporting threshold
91. What is the definition of a respondent bank?
- A. A bank for which another financial institution establishes, maintains, administers or manages a correspondent account
  - B. A bank that provides international services to another local financial institution
  - C. A foreign bank that does not have a permanent staff
  - D. A bank that is not subject to any regulation
92. What are the three classic gateways for international cooperation and sharing?
- A. Mutual legal assistance treaties (MLATs)
  - B. Law enforcement's use of grand jury subpoenas
  - C. Exchange of information between financial intelligence units (FIUs)
  - D. Exchange of information between supervisory agencies
93. What are three of the recommended ways to respond to a law enforcement inquiry?
- A. Cooperate with the law enforcement inquiry as much as possible.
  - B. Respond to all formal requests for information as promptly and thoroughly as possible, unless there is a valid objection that can and should be made.
  - C. Ensure that all communication, written and oral, is funneled through a centralized place.
  - D. Guard against unwarranted publicity by resisting all inquiries and requests whenever possible.

94. What three steps should be taken when there is a criminal investigation that is targeting the bank itself?
- A. The senior management and the Board of Directors should be notified and kept apprised of the progress of the investigation.
  - B. The bank should consider retaining experienced outside counsel to assist the bank in responding to the investigation.
  - C. The bank should immediately go to the media and explain why it has done nothing wrong.
  - D. The relevant employees of the bank should be notified of the existence of the investigation and should be given instructions as to what to do and how to act.
95. When a financial institution is responding to a formal criminal investigation by a law enforcement agency, what is the primary purpose of requiring information going through a central point within the institution?
- A. Ensure that nothing damaging to the financial institution gets released.
  - B. Ensure that responses are timely and thorough and that privileged material is not inadvertently handed over.
  - C. Ensure that the employees of the institution do not divulge information that would breach the privacy rights of customers.
  - D. Ensure that there is one person who can adequately and thoroughly apprise the Board of Directors of the progress of the investigation.
96. When a financial institution is served with a search warrant by a law enforcement agency, what are three things that the employees of the institution should do?
- A. They should not release any documents until the institution's outside counsel arrives on the scene.
  - B. They should cooperate fully with the law enforcement agents and remain calm and polite.
  - C. They should try to obtain an inventory of the materials that the law enforcement agents take from the institution.
  - D. They should review the warrant to determine its scope.
97. When should a financial institution consider retaining an experienced outside counsel for assistance?
- A. Whenever the institution receives a subpoena from any law enforcement agency
  - B. When the institution itself appears to be the target of a criminal investigation
  - C. When law enforcement appears to be focused on the accounts of a very good and long-standing customer of the institution
  - D. When the banking agencies criticize the adequacy of the institution's AML monitoring procedures

98. When should a compliance officer recommend that a financial institution conduct an internal investigation? (Choose three.)
- A. When there is a suspicion that an employee is conspiring with a long-term customer to launder money through the bank
  - B. When several customers open separate accounts at different branches but with the same contact information
  - C. When the bank's regulatory agency recommends changes to the AML policy
  - D. When a long-term employee decides to take only intermittent vacation days but not two weeks in a row, per bank policy
99. What are three practical tips in interviewing employees with regard to an unusual or suspicious transaction they have witnessed?
- A. Interview the employees as soon after the occurrence as possible in order to ensure that their memories are fresh.
  - B. Try to put the employees at ease during the interview and start with relatively easy, noncontroversial questions before getting into more sensitive matters.
  - C. Use open-ended questions for the employees in order to ensure that the questions do not dictate what the expected answer is.
  - D. Control the interview as much as possible in order to attempt to resolve the matter quickly and uncover the wrongdoer.
100. With regard to exchanges of information between FIUs of different countries, what are three controlling principles?
- A. Sharing between FIUs should be permitted only if the central banks are also a party to the sharing.
  - B. The sharing of information should be done as freely as possible on the basis of reciprocity.
  - C. The exchange of information should take place as informally and as rapidly as possible.
  - D. Differences in the definition of offenses should not impede the free exchange of information.

101. Rick is the AML compliance officer for a small bank that had AML difficulties and is operating under a deferred prosecution agreement with the federal government. The FBI approaches Rick and requests that the bank maintain an account the FBI is examining so that the FBI can monitor continuing activity. What two things should Rick do?
- A. Ask that the request be submitted in writing.
  - B. Ensure that the request is from someone with the appropriate authority.
  - C. Ask the board of directors to approve keeping the account open after an internal investigation.
  - D. Keep the account open in order to avoid incurring any further disfavor with the federal government.
102. Identify three methods of money laundering in the real estate business.
- A. Using large amounts of cash to purchase property
  - B. Disguising the beneficial ownership
  - C. Using an unlicensed agent
  - D. Generating rental income
103. Identify three methods of laundering money using lawyers.
- A. Creating trusts for clients
  - B. Buying and selling property
  - C. Setting up and managing a charity
  - D. Litigating a civil case for a client
104. Roy, a BSA officer for a large financial institution, is reviewing a possible money laundering case. What are three potential red flags that should concern him?
- A. Multiple purchases and sales of property over a short period of time
  - B. High number of transactions over the Internet or by phone
  - C. Newly arrived customer from out of state opening a business account
  - D. Two or more people using the same identification

105. Jim, an AML officer for a casino, identifies a number of potential red flags involving customers. Which should be the most troublesome?
- A. A customer purchases a number of chips, plays for a short period of time and wants to wire the proceeds of the chips to another casino in a foreign country.
  - B. A customer gambles for an extended period of time and wants to convert his chips into a check issued by the casino.
  - C. A customer gambles for an extended period of time and wants to convert his chips into cash by the casino.
  - D. A customer asks to go into the high-stakes section of the casino but does not appear to know the rules of the game he selects to play.
106. What is nesting?
- A. When a respondent bank is providing upstream correspondent services to other financial institutions
  - B. When a respondent bank is providing downstream correspondent services to other financial institutions
  - C. When a bank has many common customers with other local banks
  - D. When customers have accounts with many local banks
107. A financial institution is concerned about the possibility of the proceeds from human trafficking being funneled through the institution. What are three things the institution should look out for?
- A. Multiple wire transfers, often below the reporting thresholds, sent from foreign countries
  - B. Multiple, unrelated individuals sending wires to the same beneficiary
  - C. Accounts for foreign workers for which the employment agency is the custodian for the accounts
  - D. A group of four women who come into the financial institution to open separate accounts
108. A new products manager wants to propose a product involving prepaid cards but the AML officer sees some problems. What would be three risks that the AML officer might raise?
- A. The new product would enable customers to move funds around the world quickly.
  - B. The product can be reloaded and used anonymously.
  - C. There might be an influx of new customers who have not been vetted seeking to use the product.
  - D. The cards could be used as a substitute for bulk-cash smuggling.

109. Identify three key aspects of OFAC sanctions that have extraterritorial reach.
- A. Restricting travel by U.S. citizens to certain countries
  - B. Economic and trade sanctions based on U.S. foreign policy
  - C. Freezing foreign assets under U.S. jurisdiction
  - D. Blocking people on the Specially Designated Nationals and Blocked Persons List
110. Identify three key roles of regional FATF-style bodies.
- A. Writing the FATF 40 Recommendations
  - B. Publishing periodic typology reports
  - C. Actively participating in identifying AML technical assistance needs
  - D. Assisting in the FATF mutual evaluation process
111. Jim, an AML expert for a large bank, is reviewing some questionable customer account activity. What three scenarios should concern him the most in terms of possible AML red flags?
- A. A customer who threatens an employee in an effort to discourage required record keeping
  - B. Transaction a customer has with a country whose location is unfamiliar to the AML expert
  - C. Corporate account that shows high velocity of cash deposits and wire transfer withdrawals always leaving a low month-end balance
  - D. Employee who complains about having to file numerous reports to FinCEN
112. Identify three key aspects of delivering targeted training for different audiences and job functions.
- A. Determining whether to focus on real or hypothetical case studies
  - B. Determining how to provide the training
  - C. Determining the focus of the training
  - D. Determining whom to train

113. What are three initial things that a law enforcement investigator should consider in following up on an STR submitted by a financial institution?
- A. Identify potentially suspicious activity and any specified unlawful activity.
  - B. Trace the source and ownership of illegal money through all appropriate accounts.
  - C. In cross-border cases, seek international assistance.
  - D. Consider providing immunity to the target of the investigation to get more information quickly.
114. Jack, the AML officer for a financial institution, is confronted with reports that several bank employees have been assisting suspected money launderers. What three things should Jack consider doing to follow up on these reports?
- A. Determine whether the employees have been unduly promoted within the bank.
  - B. Determine whether the employees are living a lavish lifestyle.
  - C. Determine whether the employees may have been assisting the customers in hiding the ultimate beneficiaries of their accounts.
  - D. Determine whether the employees are involved in an excessive number of unresolved exceptions.
115. Suzy, the AML compliance officer for a large financial organization, is asked by her board of directors to review how best to protect the confidentiality of STRs submitted by the organization and the confidential information contained therein. What are three things she should consider?
- A. Ensure that employees know how to retrieve STRs by the name of the customer quickly and efficiently.
  - B. Ensure training of employees so that they do not inadvertently inform, or tip off, the targeted customer of the filing.
  - C. Ensure strong record-keeping procedures to segregate information pertaining to STRs and to maintain their confidentiality.
  - D. Ensure that procedures are in place to promptly and appropriately respond to requests for copies of filed STRs.
116. What three initial actions should a financial institution take in responding to red flags that indicate that a customer is laundering money through his or her accounts?
- A. Identify and review internal transactions engaged in by the customer.
  - B. Perform an Internet investigation focused on the customer, including a review of court records.
  - C. Confront the customer about the possible abuse of his or her accounts.
  - D. Compare the income generated by the customer with comparable businesses in the area.

117. The compliance officer of a financial institution has just received an extensive law enforcement subpoena focusing on the potential inadequacy of the institution's AML program. What three steps should the compliance officer take?
- A. He or she should advise the employees to maintain the confidentiality of all STRs.
  - B. He or she should notify the board of directors and senior management of the financial institution of the subpoena and its focus on the institution.
  - C. He or she should consider advising the institution to retain outside counsel experienced in this area.
  - D. He or she should consider providing law enforcement with the results of any internal investigation conducted by the institution.
118. What three factors could cause a financial institution to update its existing AML program?
- A. The launch of a new product
  - B. The acquisition of another financial institution
  - C. The election of a new board of directors
  - D. The passage of time (e.g., 12–18 months)
119. What are three factors with regard to how and when to report an STR to the senior management and/or the board of directors of a financial institution?
- A. Whether the STRs filed are in excess of the previous year's filings
  - B. Whether the STR raises significant issues, especially in terms of reputational risk
  - C. Whether the STR indicates any compliance deficiencies
  - D. Whether the STR is indicative of any significant AML trends
120. Diane, the AML compliance officer for a large financial institution, uncovers a serious case of potential money laundering being conducted through a number of related accounts. What three factors should she consider in deciding whether or not to close the accounts?
- A. Whether the account holder is a close associate of any of the members of the board of directors
  - B. Whether the alleged money laundering activity is occurring in all of the accounts or just some of the accounts
  - C. The legal basis for closing the accounts
  - D. The reputational risk to the institution if the accounts are maintained

**ANSWERS**

1. A	21. A, B, C	41. A	61. C	81. A	101. A, B
2. B	22. A, C, D	42. D	62. D	82. B, C	102. A, B, C
3. A	23. D	43. A	63. D	83. A, B, C	103. A, B, C
4. B, C, D	24. A, C	44. D	64. B	84. B	104. A, B, D
5. A, C	25. C	45. A, B, D	65. A	85. A, C	105. A
6. D	26. A	46. A	66. A, B, D	86. C	106. B
7. C	27. D	47. A, B, D	67. D	87. A, B, C	107. A, B, C
8. B	28. D	48. A	68. B	88. B	108. A, B, D
9. A, B, D	29. C	49. C	69. C	89. A, B, D	109. B, C, D
10. A, C, D	30. A	50. A	70. A	90. B, C, D	110. B, C, D
11. A	31. B	51. C	71. C	91. A	111. A, B, C
12. C	32. C	52. B	72. A	92. A, C, D	112. B, C, D
13. D	33. A	53. A, B, D	73. C	93. A, B, C	113. A, B, C
14. B, C, D	34. C	54. A	74. A, B, C	94. A, B, D	114. B, C, D
15. C	35. C	55. D	75. C	95. B	115. B, C, D
16. A	36. A	56. A, B, C	76. B	96. B, C, D	116. A, B, D
17. C, D	37. B	57. C	77. A	97. B	117. B, C, D
18. B	38. A	58. C	78. A, B, C	98. A, B, D	118. A, B, D
19. B	39. B	59. A, B, C	79. A, B, D	99. A, B, C	119. B, C, D
20. A, B, D	40. B	60. A	80. B	100. B, C, D	120. B, C, D

**NOTES:**

[illegible]

[illegible]

# Chapter 7

## Guidance Documents and Reference Materials

**T**his section cites several CAMS Examination supporting documents and reference materials. It also suggests websites and periodicals that offer additional supporting material. Several international bodies that are focused on AML/CFT have published valuable guidance documents and reference materials that are helpful in preparing for the CAMS Examination.

For study purposes, generally the reference documents have an introduction, putting the material in context and, in some cases, describing the methodology behind their production. For example, in each of FATF's Risk-Based Approach Guidance documents, the purpose of the risk-based approach is explained in the opening chapter. The core material then describes the specific AML risks that are the focus of the guidance and describes the best practices for mitigating those risks. It is this core material that is examined in the CAMS Examination.

Two documents above all others (FATF's 40 Recommendations and Interpretive Notes) should receive particular study from CAMS candidates. It is highly advised to download the free .pdf versions available from the FATF website to keep with your other CAMS study materials. The 40 Recommendations are the basic elements of every AML regime at the national and financial institution levels and most of the other materials build off specific aspects of this foundation.

## Guidance Documents and Reference Materials

---

(PDF Version: Copy and paste links into web browser to locate referenced material.)

- I. Financial Action Task Force (FATF):** <http://www.fatf-gafi.org>
  - **The Forty Recommendations and Interpretative Notes (February 2012)**  
[http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc\(fatf\\_releasedate\)](http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate))
- II. Basel Committee on Banking Supervision:** [www.bis.org](http://www.bis.org)
  - **Customer Due Diligence for Banks** (October 2001)  
[www.bis.org/publ/bcbs85.htm](http://www.bis.org/publ/bcbs85.htm)
  - **Consolidated KYC Risk Management** (October 2004)  
[www.bis.org/publ/bcbs110.pdf](http://www.bis.org/publ/bcbs110.pdf)

- **Sound Management of Risks Related to Money Laundering and Financing of Terrorism** (January 2014)  
<http://www.bis.org/publ/bcbs275.htm>
- **General Guide to Account Opening** (February 2016)  
<http://www.bis.org/bcbs/publ/d353.htm>
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers**  
<http://www.bis.org/publ/bcbs154.pdf>
- **Sharing of Financial Records Between Jurisdictions in Connection With the Fight Against Terrorist Financing** (April 2002)  
[www.bis.org/publ/bcbs89.pdf](http://www.bis.org/publ/bcbs89.pdf)
- **General Guide to Account Opening and Customer Identification** (February 2003) (Attachment to Basel Committee publication “Customer due diligence for banks”)  
[www.bis.org/publ/bcbs85annex.htm](http://www.bis.org/publ/bcbs85annex.htm)
- **Compliance and the Compliance Function in Banks**  
<http://www.bis.org/publ/bcbs113.pdf>

### III. FATF-Style Regional Bodies

#### A. Asia Pacific Group on Money Laundering

[www.apgml.org](http://www.apgml.org)

- **Methods and Typologies**  
<http://www.apgml.org/methods-and-trends/page.aspx?p=a4a11dca-75f2-4dae-9c25-6215103e56da>

#### B. Caribbean Financial Action Task Force [www.cfatf.org](http://www.cfatf.org)

- **Typologies Exercises**  
<https://www.cfatf-gafic.org/index.php/documents/typologies>

#### C. Committee of Experts on the Evaluation of AML Measures and the Financing of Terrorism (MONEYVAL)

<http://www.coe.int/t/dghl/monitoring/moneyval/>

#### D. Eastern and Southern African Money Laundering Group

[www.esaamlg.org](http://www.esaamlg.org)

- Typologies—<http://www.esaamlg.org/reports/typologies.php>

#### E. Eurasian Group on Combating Money Laundering and Financing of Terrorism

<http://www.eurasiangroup.org/>

- Typologies—[http://www.eurasiangroup.org/typology\\_reports.php](http://www.eurasiangroup.org/typology_reports.php)

#### F. Grupo de Acción Financiera Internacional de Latin America (GAFILAT)

<http://www.gafilat.org/?id=inicio&lang=en>

- G. Intergovernmental Action Group Against Money Laundering in Africa (GIABA)** <http://www.giaba.org/>
- Typologies—<http://www.giaba.org/reports/typologies/reports.html>
- H. Middle East and North Africa Financial Action Task Force (MENAFATF)** [www.menafatf.org](http://www.menafatf.org)
- Typologies—<http://www.menafatf.org/TopicList.asp?cType=typ>
- IV. United Nations (U.N.):** <http://www.un.org>
- **Model legislation on money laundering and financing of terrorism**  
<http://www.unodc.org/unodc/en/money-laundering/Model-Legislation.html?ref=menuside>
  - **U.N. Security Council Resolutions on Terrorism**  
<http://www.un.org/en/counterterrorism/index.shtml>
- V. International Money Laundering Information Network:** [www.imolin.org](http://www.imolin.org)
- VI. European Union:** <http://europa.eu/>
- 4th EU Money Laundering Directive (Directive (EU) 2015/849 of the European Parliament and the Council of May 20, 2015)  
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849>  
(*N.B. – this repeals the 3rd EU Directive*)
  - 3rd EU Directive 2005/60/EC of the European Parliament and of the Council (October 2005 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005L0060:EN:NOT>)  
(*N.B. This directive expands on the 2nd EU Directive 2001/97/EC of the European Parliament and of the Council on Prevention of the Use of the Financial System for the Purpose of Money Laundering (December 2001).*)
- VII. Egmont Group of Financial Intelligence Units:** [www.egmontgroup.org](http://www.egmontgroup.org)
- 100 Sanitised Cases [http://www.egmontgroup.org/library\\_sanitized\\_cases.html](http://www.egmontgroup.org/library_sanitized_cases.html)
- VIII. Wolfsberg Group:** [www.wolfsberg-principles.com](http://www.wolfsberg-principles.com)
- **Wolfsberg AML Principles for Correspondent Banking**  
(Issued November 2002, revised 2014)  
<http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Correspondent-Banking-Principles-2014.pdf>
  - **Wolfsberg Statement on the Suppression of the Financing of Terrorism** (January 2002)  
[http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg\\_Statement\\_on\\_the\\_Suppression\\_of\\_the\\_Financing\\_of\\_Terrorism\\_\(2002\).pdf](http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_(2002).pdf)

- **Wolfsberg AML Principles on Private Banking** (Issued in 2002, Revised in 2012)  
<http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Private-Banking-Principles-May-2012.pdf>
- **Wolfsberg Statement on AML Screening, Monitoring and Searching 2009**  
[http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg\\_Monitoring\\_Screening\\_Searching\\_Paper\\_\(2009\).pdf](http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Monitoring_Screening_Searching_Paper_(2009).pdf)
- **Wolfsberg Anti-Corruption Guidance** (2011)  
[http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg%20Anti%20Corruption%20Guidance%20Paper%20August%2018-2011%20\(Published\).pdf](http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg%20Anti%20Corruption%20Guidance%20Paper%20August%2018-2011%20(Published).pdf)

## Other Websites with Helpful AML Material

---

CAMS qualified professionals will routinely consult the websites of their home regulators. However, there are other websites that contain helpful AML materials.

### **Association of Certified Anti-Money Laundering Specialists**

[www.ACAMS.org](http://www.ACAMS.org)

### **Australian Transaction Reports and Analysis Centre (AUSTRAC)**

[www.austrac.gov.au](http://www.austrac.gov.au)

### **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**

[www.fintrac.gc.ca](http://www.fintrac.gc.ca)

### **International Monetary Fund**

[www.imf.org/external/np/exr/facts/aml.htm](http://www.imf.org/external/np/exr/facts/aml.htm)

### **UK Financial Conduct Authority**

<https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing>

### **U.S. Financial Crimes Enforcement Network home page**

[www.fincen.gov](http://www.fincen.gov)

### **U.S. Federal Financial Institutions Examination Council (FFIEC)**

#### **Bank Secrecy Act/Anti-Money Laundering InfoBase**

[http://www.ffiec.gov/bsa\\_aml\\_infobase/default.htm](http://www.ffiec.gov/bsa_aml_infobase/default.htm)

### **U.S. Office of Foreign Assets Control (OFAC)**

<https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>

### **World Bank**

[www.worldbank.org](http://www.worldbank.org)

## **AML-Related Periodicals**

---

### **ACAMS Today**

A quarterly magazine for ACAMS members providing stories from the AML workplace and current global issues and developments on money laundering.  
<http://acamstoday.org/wordpress/>

### **ACAMS MoneyLaundering.com**

A monthly newsletter focusing on current global, legal, regulatory and enforcement issues and other money laundering-related news, analysis and guidance.  
[www.moneylaundering.com](http://www.moneylaundering.com)

### **Money Laundering Bulletin**

A UK-based newsletter published 10 times per year addressing issues on money laundering practices, policing efforts and the anti-laundering systems of various industries.  
<http://www.moneylaunderingbulletin.com/>

### **ABA Bank Compliance**

The American Bankers Association's monthly magazine dealing with legal, regulatory and compliance issues and information.  
<http://www.aba.com/Products/bankcompliance/Pages/default.aspx>

**NOTES:**

[illegible]

# Contact Us

## UNITED STATES

### Chicago

500 W. Monroe Street

Suite 28

Chicago, IL 60661

T: +1.305.373.0020

T: +1.866.256.8270

F: +1.305.373.7788

F: +1.305.373.5229

E: [info@acams.org](mailto:info@acams.org)

## ASIA PACIFIC

### Hong Kong

23/F, One Island East

18 Westlands Road

Quarry Bay, Hong Kong S.A.R.

T: +852.3750.7684 | 7658 | 7694

F: +852.3010.1240

E: [apac@acams.org](mailto:apac@acams.org)

## EUROPE

### London

Level 25 | 40 Bank Street

Canary Wharf

London | E14 5NR

United Kingdom

T: +44.20.3755.7400

E: [europa@acams.org](mailto:europa@acams.org)

[acams.org](http://acams.org)

A PUBLICATION OF

**ACAMS**  TM