Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Financial Services | the way we see it

The Growing Threat of Money Laundering

The significant role financial services institutions can play in curbing money laundering activities

People matter, results count.

Contents

1 Highlights

The world economy is heavily affected by money that is illegally acquired and used for illegitimate purposes. Large sums of money are laundered every year, posing a threat to the global economy and its security.

Financial services institutions such as banks, non-banking financing companies, insurers, and capital market firms are generally the most favored channels through which illicit money is laundered across the globe. Many financial services institutions may be associated with money launderers unknowingly, which is a primary reason that financial firms are subjected to stringent anti-money laundering (AML) regulations to track the trail of illegally-sourced earnings.

This paper provides a brief overview of the evolution of money laundering and common money laundering tactics around the world, and discusses the implications of money laundering activities on the global economy and financial services industry. The analysis also describes key anti-money laundering regulations and regulatory bodies, and shows how financial services firms can leverage technology to comply with increasing AML regulations and control the money laundering menace.

2 Introduction

The main drivers of money laundering are: Corruption, organized crime, financial fraud, arms dealing, drugs/sex trade, and terrorist financing.

Money laundering has been affecting the global economy for many years. Large sums of money are laundered every year, posing a threat to the global economy and its security. Money laundering encompasses illegal activities that are used to make illegally-acquired funds appear legal and legitimate. Illegal sources of money and financial assets are often disguised and concealed using a smoke screen of deceptive practices. The main drivers of money laundering are:

- Corruption,
- Organized crime,
- Financial fraud,
- Arms dealing,
- Drugs/sex trade, and
- Terrorist financing.

The typical drivers for money laundering are similar across the globe. However, there are regional variations in terms of what primarily drives money laundering. For example, corruption is one of the primary drivers for money laundering in developing nations due to higher levels of corruption overall. Across the globe, organized crime, drugs, and smuggling are some of the major contributors to money laundering.

2.1. Stages Involved in Money Laundering

Money laundering is the process used to legitimize illegal funds by concealing or disguising the true source of financial assets. Organized crime groups use laundered money to profit from illegal activities and sometimes even finance terrorist activities. The methods used for money laundering can vary in complexity and sophistication, though the following stages have been frequently observed in the process used by money launderers[1]:

Placement

Placement involves placing unlawful cash proceeds with banks and other financial institutions using deposits, wire transfers, or other financial instruments.

Layering

Layering involves converting the proceeds of illegal activities into other forms and creating complex layers of financial transactions. Money launderers make it difficult to trace the source and ownership of financial assets by buying and selling stocks, commodities, and property. The intent behind layering is to blur the audit trail of the financial sum involved.

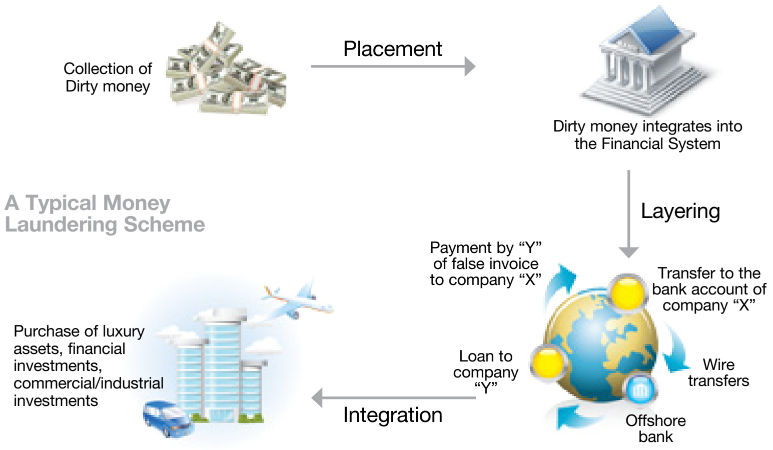
Integration

Integration attempts to provide a seemingly legal explanation for the placed and layered financial assets. It is used to distribute laundered funds back to the criminals. Various false transactions and fake invoices are used to enable the transfer of this money. Exhibit 1 explains a typical process of money laundering and its stages.

[1] Board of Governors of the Federal Reserve System

The act of money laundering generally involves three steps: Placement, Layering, and Integration.

Exhibit 1: Stages Involved in Typical Money Laundering Scheme


Collection of Dirty money
Placement
Dirty money integrates into the Financial System
A Typical Money Laundering Scheme
Layering
Payment by "Y" of false invoice to company "X"
Transfer to the bank account of company "X"
Wire transfers
Loan to company "Y"
Offshore bank
Purchase of luxury assets, financial investments, commercial/industrial investments
Integration

Source: Terrorist Financing Models, FINTRAC, June 2009

2.2. Evolution of Money Laundering: Common Tactics

Money laundering has evolved over the years, with the oldest methods based on paper and hard currency. However, the advent of modern technology has given rise to a whole new range of sophisticated methods.

In today's environment, money laundering is generally undertaken through four primary methods:

- Loan-back money laundering,
- Front company,
- Trusts, and
- Black Market Currency Exchange (BMCEs)[2]

The most common tactics of money laundering in today's world include: Loan-back money laundering, front company, trusts, and Black Market Currency Exchange schemes.

Exhibit 2: Evolution of Money Laundering Techniques

Hawala: (India)

- In hawala, funds are moved between individual "hawaladars" which collect funds at one end of the operation and other hawaladars that distribute the funds at the other end

Third Party Cheques:

- Utilizing counter cheques or banker's drafts drawn on different institutions and clearing them via various third-party accounts
- Since these are negotiable in many countries, the nexus with the source money is difficult to establish

Casinos: (North America)

- The cash intensive nature of the casino business and the size of transaction frequency and volumes had made it vulnerable to money laundering
- North America accounted for around 50% of the global casino market even as late as 2009

Cyber Crime:

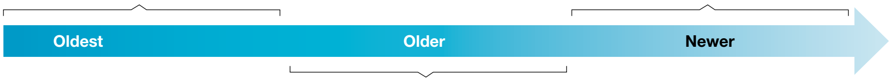
- Cyber crimes such as identity theft, illegal access to e-mail, and credit card fraud are coming together with money laundering and terrorist activities

Open Securities Market:

- Laundering is possible due to the instruments like hedge funds and participatory notes which have very limited disclosures as to the source

Insurance Sector:

- If a money launderer is able to move funds into an insurance product and receive a payment made by an insurance company then he or she will have made the funds appear legitimate



Structuring:

- Depositing of cash or purchasing of bank drafts at various institutions by several individuals, or carrying out of transactions below reporting thresholds

Credit Cards:

- Creating credit on a card by paying cash on the card allowing the credit to be converted to cash

Source: Capgemini Analysis, 2011; Financial Action Task Force on Money Laundering

[2] Primary source is the Black Market Peso Exchange (BMPE)

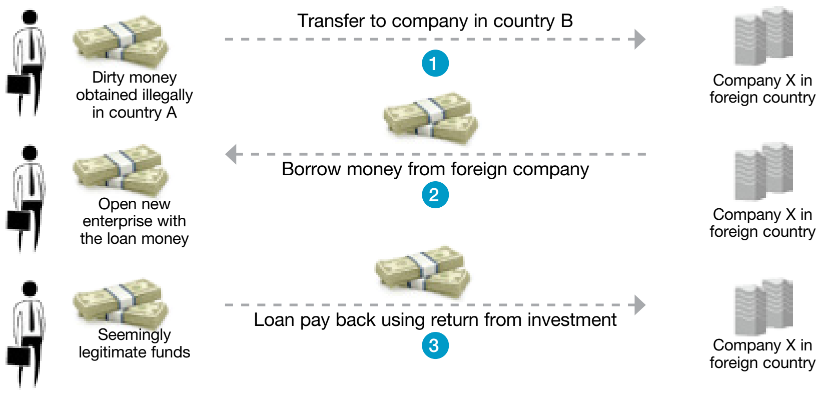
Loan-Back Money Laundering

The main tactic behind this method of laundering money is that the person borrows their own criminal funds, either directly or indirectly, without other people noticing. This allows the money launderer to deceive authorities and launder the funds.

Illicitly earned money in a particular country is transferred to a company in another country. The illegal money is generally deposited in smaller amounts into bank accounts of foreign companies. These companies are typically chosen in countries that have more bank secrecy laws and less chance of transactions getting noticed or being traced back.

Once the amount has been transferred to the foreign company, the originator of the transfer or an affiliate receives a loan from the foreign company to open a company in the home country. Thus, the money that is earned illegally is placed into the system, layered, and then integrated to make it appear legal.

Exhibit 3: Loan-Back Money Laundering Scheme

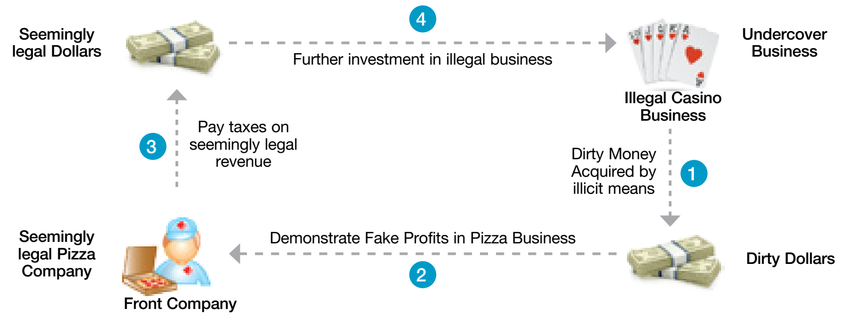

Dirty money obtained illegally in country A
Transfer to company in country B
1
Company X in foreign country
Open new enterprise with the loan money
Borrow money from foreign company
2
Company X in foreign country
Seemingly legitimate funds
Loan pay back using return from investment
3
Company X in foreign country

Source: Capgemini Analysis, 2011

Front Company

Money launderers often use a front company, also called a shell company, to conceal the true beneficial owners who are seeking to profit from the laundered funds. Generally, a front company mixes the proceeds of illegal activities with legitimate funds to hide the illegal proceeds. The front company provides goods at subsidized rates, showing false profits for the company. As the front company has access to illicit funds, they mix the earnings from legal and illegal methods to make them look legal. The profit earned by the front company is further used to promote the illegal activities running in the background.

Exhibit 4: Money Laundering using a Front Company

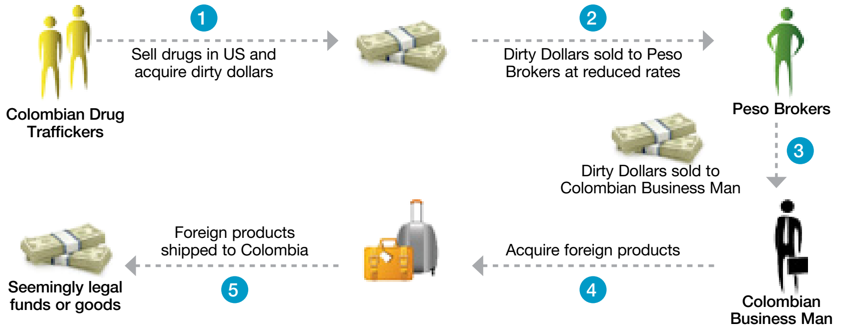

Seemingly legal Dollars
4
Further investment in illegal business
Undercover Business
Illegal Casino Business
3
Pay taxes on seemingly legal revenue
Dirty Money Acquired by illicit means
1
Seemingly legal Pizza Company
Demonstrate Fake Profits in Pizza Business
2
Dirty Dollars
Front Company

Source: Capgemini Analysis, 2011; The Asia/Pacific Group of Money Laundering

Trusts

Trusts are also sometimes used to hide assets from legitimate creditors, protect property from seizure under judicial action, or to mask the various links in the money flows associated with laundering or tax evasion schemes. The payments to a trust's beneficiaries could be used in the laundering process because these payments do not have to be justified as a payment for a transfer of assets or service rendered.

Exhibit 5: Money Laundering using BMPE


1
Sell drugs in US and acquire dirty dollars
2
Dirty Dollars sold to Peso Brokers at reduced rates
Colombian Drug Traffickers
Peso Brokers
3
Dirty Dollars sold to Colombian Business Man
Foreign products shipped to Colombia
Acquire foreign products
Seemingly legal funds or goods
5
4
Colombian Business Man

Source: Capgemini Analysis, 2011

Black Market Currency Exchange

Black Market Currency Exchange is a term used to refer to the black market in foreign exchange of any country, and is commonly found in Columbia. These black markets are often found in countries where currencies are unstable, and provide launderers with the opportunity to conduct financial transactions in foreign and domestic currencies.

For instance, in Columbia, the drug cartels have been known to use the Black Market Peso Exchange system to sell foreign currencies to dealers at deeply discounted values. In this way, the drug cartels convert drug revenue from a foreign country into usable pesos in Colombia. The currency dealers in turn sell these currencies to individuals and businesses in need of such foreign currency for business or personal reasons, making a substantial profit on the exchange rates. The dirty money now reaches the realm of legitimate commerce as these prior transactions are not recorded and are conducted unofficially.

2.3. Money Laundering through New Payment Systems

Increasing proliferation of new non-cash payment methods such as prepaid cards, internet payments, and mobile payments has opened up new gateways for money launderers. The rapid speed of transactions, coupled with minimal face-to-face interaction between the person initiating the transaction and the service provider, makes these new payment modes vulnerable to money laundering activities.

Some of the vulnerabilities in the prepaid cards can be tied to the fact that many of these instruments can be issued in 'country X' and used in 'country Y', and vice versa. These prepaid cards, which can be used across borders and do not require extensive customer identification for issuance, are at the highest risk of misuse by launders. The use of prepaid cards not only provides an easier vehicle for money laundering but also increases the risk for illegal activities using unaware or unwilling account holders. Additionally, various card versions are available in the market today which can be loaded online, thus making it more vulnerable to money laundering and terrorist financing activities.

Internet payment services, as well as mobile payments, share the same basic characteristics of quick transaction speeds and lack of face-to-face interaction between the related parties, making them vulnerable to money laundering activities.

The Financial Action Task Force in its October 2010 report identified several cases of money laundering using new payment methods[3]:

Indentified Misuse of Prepaid Cards for Money Laundering
In 2007, certain steroids were sold illegally over the internet in the U.S. The buyer would load the seller's prepaid card to complete the purchase, thus allowing the sale of illegal substances.

In 2009, a group of criminals were charged for a drug trafficking racket under which they supplied drugs to people serving time in prison. The proceeds for drug sales were received by the defendants by having their prepaid cards loaded directly by the relatives of the prisoners outside the prison.

Indentified Misuse of Internet Payment Services for Money Laundering
In 2010, the German Financial Intelligence Unit reported several cases of money laundering under which phishing transfers were made to a financial agent's account. In return, the financial agent purchased low-value cash vouchers from internet payment service providers and sent the voucher details back to the instructor. These coupons were used by the money launderer to make internet payments for purchase of certain goods and services.

Indentified Misuse of Mobile Payments Services for Money Laundering
In April 2010, a case was reported in the Cayman Islands in which an individual used stolen credit cards to purchase credits for mobile payments. These phone credits were later sold under mobile peer-to-peer payments.

[3] Money Laundering using New Payment Methods, October 2010

2.4. Recent High Profile Cases of Money Laundering

2G Spectrum Allocation Scam in India

The 2nd generation (2G) spectrum allocation scam of 2008, under the ruling of the Congress party-led United Progressive Alliance (UPA) government, was arguably one of the historically largest corruption scams in India. Under this scam, senior government officials were accused of issuing over 1,230 spectrum licences to approximately 85 telecom companies at artificially discounted prices[4]. According to the Comptroller and Auditor General report, the spectrum scam is believed to have caused nearly US$40bn of loss to the exchequer.

Charges under the Prevention of Money Laundering Act and the Foreign Exchange Management Act were filed for this scandal and several major arrests were made. The investigation is still ongoing. The Enforcement Directorate of India (ED) has claimed that the 2G scam's money trail is linked to around 10 countries and the case has international ramifications.

Madoff Investment Scandal

Bernie Madoff, the founder of the investment firm Bernard L. Madoff Investment Securities LLC, was charged with 11 different criminal offences including fraud, theft, perjury, false filing with the SEC, and money laundering in March 2009.

Madoff had committed a series of crimes over more than 20 years and was ultimately sentenced to 150 years in prison along with restitution of US$170bn. Out of the 150 years of imprisonment, approximately 50 years of the sentence are related to various money laundering crimes that he had committed.

[4] "Corrupt politicians in India", Blitz, http://www.weeklyblitz.net/1663/corrupt-politicians-in-india

[5] 2G accused move court to have TRAI report on record, Business Standard, http://www.business-standard.com/2gscam/news/2g-accused-move-court-to-have-trai-reportrecord/146071/on

3 Business Implications of Money Laundering

In today's global economy, money laundering activities can have a significant negative macroeconomic impact, especially on developing countries with weak anti-money laundering regulations. Once illicitly earned money enters into a particular economy's financial system, it has the ability to destabilize the economic system and indirectly promote negative social and legal ills such as tax evasion, corruption, drug trading, and terrorism.

3.1. General Implications of Money Laundering

Overall, the negative implications of money laundering on a particular nation can be broadly grouped into three main categories as described below.

Economic Impact

Money laundering goes hand-in-hand with tax evasion and duty evasion (which is the non-payment of import and export duties by smuggling goods in and out of a nation). Such activities deprive public service departments of important revenue sources.

Additionally, money launderers have a tendency to direct and redirect their money from one asset class to another. This creates a complex cycle of financial transactions that hides the illegal origin of the money. Money launderers disguise their illegal money and park it in places where the possibility of being caught is minimal, rather than making profits with it. Such logic-defying investment activities have the ability to destabilize the overall financial system by weakening investor confidence due to unnecessary volatility, especially when the fund inflows and outflows of these laundering activities are disproportionately high.

Another negative consequence of money laundering activities for a nation is the increase in interest rates and foreign exchange volatility on account of irregular and unanticipated capital flows, which makes policy making an arduous task for the government[6].

Legal Impact

Money laundering and criminal activities form a vicious cycle. The quest to legalize illicit earnings spawns money laundering, which in turn provides the required financial boost for these illegal activities to survive. Several large-scale illegal activities such as arms dealing, organized crime, terrorist financing, as well as drug and sex trafficking, do not just drive money laundering but thrive on it. There generally exists a direct relation between countries having weak anti-money laundering regulations and prevalence of such illegal and criminal activities. However, in certain countries which have purposefully relaxed anti-money laundering regulations to attract capital, the negative effects of the increased illegal activities may not be felt in their own territory, but could enable illegal activities in other countries.

[6] The consequences of money laundering and financial crime, U.S. Dept of State, 2001

Social Impact

Criminals launder money to circulate their illicit earnings, which then provides the firepower to grow the illegal business. The social impact of strong illegal businesses includes increased drug addiction, rampant corruption, and criminals empowered with economic powers.

3.2. Implications Specific to the Financial Services Industry

Money laundering does not necessarily involve financial services institutions. However, banks (including non-banking financing companies, insurance companies, and capital market firms) have generally been the favored channel for laundering illicit money across the globe[7].

Financial services institutions with weaker anti-money laundering laws are generally more exposed to legal, regulatory, and reputational risks.

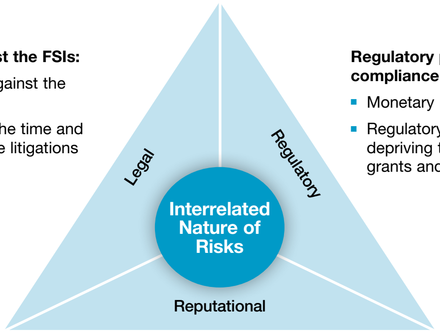
The proximity of money launderers to the financial services industry, and the fact that most financial services institutions can become subject to laundering even unknowingly, makes financial firms subject to stringent national as well as regional or even global anti-money laundering regulations. It is in the best interest of financial services institutions to have effective risk governance practices including internal controls and regular audit checks to mitigate legal and regulatory consequences. Additionally, financial services institutions tainted by money laundering are exposed to operational and reputational risks.

Exhibit 6 captures the risks associated with money laundering activities for financial services institutions.

Exhibit 6: Risks of a Deficient Anti-Money Laundering System for a Financial Services Institution

Legal proceedings against the FSIs:

- Direct costs to defend against the lawsuits (attorney fees)
- Indirect costs including the time and effort spent to defend the litigations



Regulatory proceedings for non-compliance of existing AML laws:

- Monetary penalties
- Regulatory sanctions including depriving the FSI of government grants and benefits

Negative media publicity leading to adverse effects on business operations:

- Loss of investor trust (leading to loss in share value for publicly listed FSIs)
- Inability to stay competitive due to loss of confidence from customers and business partners from whom they source funds

Source: Capgemini Analysis, 2011

[7] The negative effects of money laundering on economic development, Asian Development Bank, May 2002

Regulatory Risks
Regulatory risks are the negative consequences that financial services institutions are likely to face if they don't comply with regulatory/legislative norms meant to counter money laundering activities. Some of the consequences include monetary penalties, regulatory sanctions such as depriving the institution from receiving certain government grants and benefits (coverage under the central banks' credit guarantee program), and a ban on certain operations of the firm for a defined time period.

Legal Risks
Legal risks also stem from a lack of regulatory compliance. When a financial services institution is found to be associated with money laundering activity, the firm and key stakeholders face legal proceedings on the grounds of having a deficient anti-money laundering compliance system. These litigations cost management a lot of time as well as direct financial costs to defend themselves against the claims.

Reputational Risks
Trust and integrity are the keys to success for any financial services institution. Any event that taints the firm's reputation in the form of regulatory and legal sanctions can cause serious direct as well as indirect losses to the firm. For financial services institutions, reputational risks include the inability to raise funds at competitive rates and loss of investor and customer trust leading to lost business opportunities.

Association, or even rumors of being associated, with laundering activities leads to adverse media publicity for financial services institutions with questions being raised about the integrity of the firm and its business ethics. Such negative publicity by the media aggravates the reputational damage for the tainted financial services institutions.

The propensity of money launderers to channel dirty money through mainstream and niche financial services institutions exposes these economically important institutions to serious risks. It is therefore imperative that both national and international regulatory bodies not just curb the illicit laundering activity, but also strictly monitor all financial services institutions for any wrongdoing—either deliberate or due to insufficient controls.

4 Measures to Counter Money Laundering

4.1. Anti-Money Laundering – Regulatory Landscape

Global and Regional Regulatory Bodies

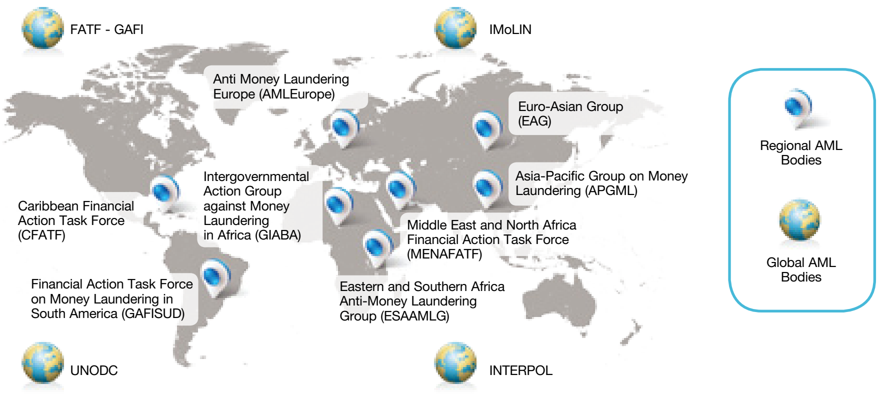
The act of money laundering can occur anywhere across the globe, where people can make money from illegal/criminal means such as corruption, drug trafficking, arms dealing, financial fraud, and organized crime. However, money launderers generally choose to operate in nations that have weaker legislations around detecting money laundering activities. It is due to the interconnected nature of the global economy that money laundering is an international problem, and global cooperation in tackling this problem is of utmost importance.

Due to the adverse macroeconomic consequences that money laundering can have—especially on developing nations—global organizations such as the International Monetary Fund (IMF) and World Bank have launched several initiatives to combat money laundering and terrorist financing activities. These initiatives can be broadly classified into four broad categories based on the project goals:

- **Raise awareness** about the negative impacts of money laundering with the leaders of various nations and inform them about various resources that they can avail to counter money laundering activities.
- **Develop a universal methodology** for AML and combating financial terrorism (CFT) to assess each country on their preparedness to address these issues.
- **Build institutional capacity** by organizing training conferences for specific AML or CFT issues and delivering technical support to countries that want to establish or improve existing AML and CFT laws.
- **Other activities** such as keeping a check on alternative remittance channels.

Overall, the international nature of money laundering has led to the formation of several global and regional regulatory bodies to deal with the threat.

Exhibit 7: Framework of Global and Regional AML Bodies


FATF - GAFI
IMoLIN
Anti Money Laundering Europe (AMLEurope)
Euro-Asian Group (EAG)
Intergovernmental Action Group against Money Laundering in Africa (GIABA)
Asia-Pacific Group on Money Laundering (APGML)
Caribbean Financial Action Task Force (CFATF)
Middle East and North Africa Financial Action Task Force (MENAFATF)
Financial Action Task Force on Money Laundering in South America (GAFISUD)
Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
UNODC
INTERPOL
Regional AML Bodies
Global AML Bodies

Source: Capgemini Analysis, 2011

The four major global anti-money laundering bodies that formulate guidelines and policies to combat money laundering activities worldwide are:

- **Financial Action Task Force (FATF):** FATF is an independent inter-governmental body that develops and promotes policies at both a national and international level in order to combat money laundering and terrorist financing. FATF has provided a list of 40 recommendations and nine special recommendations that act as the standards to counter money laundering and terrorist financing.
- **International Money Laundering Information Network (IMoLIN):** IMoLIN is an internet-based network which was developed with the cooperation of leading global anti-money laundering organizations such as FATF, UNODC, Asia-Pacific Group of Money Laundering, and the Council of Europa (among others). The main operation of IMoLIN is to assist various national governments, public and private organizations, and individuals in the fight against money laundering and terrorist financing.
- **United Nations Office of Drugs and Crime (UNODC):** UNODC's organized crime and anti-money laundering unit carries out the global program against money laundering. The basic objective of the program is to empower member states to implement anti money laundering and terrorist financing measures. The UNODC also assists members in detecting and confiscating illegal proceeds per the UN norms.
- **INTERPOL:** The primary objective of the anti-money laundering unit of INTERPOL is to increase the speed of information exchange among the financial crime investigators with the aid of global financial crime units as well as financial intelligence units.

All the above mentioned global bodies, as well as FATF-styled regional bodies, work on a collaborative basis and share information. These organizations also share information on money laundering activities with global and regional financial institutions such as the International Monetary Fund, World Bank, European Central Bank, and the Asian Development Bank to combat money laundering and terrorist financing threats.

Additionally, the need to deal with the growing problems of international money laundering and related financial crimes has led to the emergence of certain specialized government agencies, generally referred to as Financial Intelligence Units (FIUs). The primary task of FIUs is to provide continuous exchange of information between financial services institutions, jurisdictions, and other prosecuting authorities. Most FIUs across the globe are now a part of the Egmont Group, which is an informal international gathering of FIUs, wherein the member FIUs regularly meet to find ways to increase internal cooperation and areas of information exchange, training and the expertise sharing.

Local Market Anti-Money Laundering Regulations

A closer look at several national laws and regulations around anti-money laundering suggests that there has been a lot of activity around strengthening money laundering laws across the globe, especially over the past decade. Listed below are a few of the major national laws that have been enacted over the past few years:

- **The U.S.:** USA Patriot Act (2001)
- **Europe:** Third European Directive (2003)
- **China:** Law of the People's Republic of China on Anti-Money Laundering (2006)
- **Japan:** The Act on the Prevention of Criminal Proceeds (2007)
- **India:** Prevention of Money Laundering Act (2002)

Most anti-money laundering regulations across the globe, including those listed above, have three common elements[8]: Criminalization of money laundering; confiscation of criminal proceeds; and obligations of a certain range of business operators—especially financial services institutions—to take preventive measures.

[8] Japan Financial Intelligence Center Annual Report 2009

4.2. Organizational Approach to Counter Money Laundering and to Comply with Regulations

The following tools and concepts are used by financial services institutions as basic measures to address money laundering and related compliance issues.

Know Your Customer (KYC)

Various regulations from across the world mandate financial services institutions to know certain details about their customers as part of their usual process of customer acquisition. This will help protect themselves and stakeholders from potential money laundering schemes. A majority of financial services institutions have a rigid KYC compliance policy, either by law or through their own vested interest to protect themselves against reputational risks. Financial services institutions can perform checks on potential as well as existing customers to better know them and understand their sources of wealth.

Watch List Filtering

Under watch list filtering, financial services institutions screen for all parties involved in various day-to-day financial transactions. The idea behind screening these transactions is to deal with money laundering issues through a risk-based approach. Financial services institutions screen all entities and individuals against a list of high-risk individuals provided by financial intelligence units, as well as other politically exposed persons who are likely candidates for money laundering activities.

Suspicious Activity Reporting

Financial services institutions generally report any known or suspicious activity around money laundering to financial intelligence units, as well as other national/state financial crime and anti-money laundering units.

Suspicious Transaction Reporting (STR)

When a financial services institution has a strong reason to believe one of its transactions is being used to finance terrorist activities or launder money, the company is required to report the transaction to FINTRAC. Under no circumstances is the client under suspicion to know that he or she has been reported as a suspect.

Policy Formulation and Employee Training

Financial services institutions across the globe have anti-money laundering policy guidelines and minimum standards in the form of "do's" and "don'ts" for employees. In addition, most financial services employees are given training on various regulations around money laundering and their obligations to comply with the regulations.

5 The Role of Technology in Anti-Money Laundering (AML)

Technology has played a significant role in the emergence of the current global and interconnected financial system. Financial services institutions and customers have benefitted from the widespread adoption of technology, but this technological advancement has also opened up new gateways for money launderers to legalize their illicit earnings with relative ease by capitalizing on weaknesses in the financial system.

Overall, money laundering activity has evolved over the years parallel to the technological advancement of the financial system. Driven by the growing sophistication of money launderers, various national and international regulations have also evolved. With the exponential growth in financial transaction volumes it has become mandatory for financial services institutions to strengthen their anti-money laundering efforts through advanced technologies in order to alert and report any suspicious activities to regulatory bodies and internal controllers.

5.1. Evolution of the Anti-Money Laundering Solutions Landscape

The traditional first generation of anti-money laundering solutions operated on an if-then, rule-based approach to detect and alert any potential money laundering schemes. These rule-based solutions analyzed data for suspicious laundering activities based on certain user-created scenarios, which were a combination of monetary thresholds as well as existing laundering patterns. However, as the sophistication of money laundering evolved over the years, conspirators began outwitting these solutions and the need for second generation anti-money laundering solutions emerged.

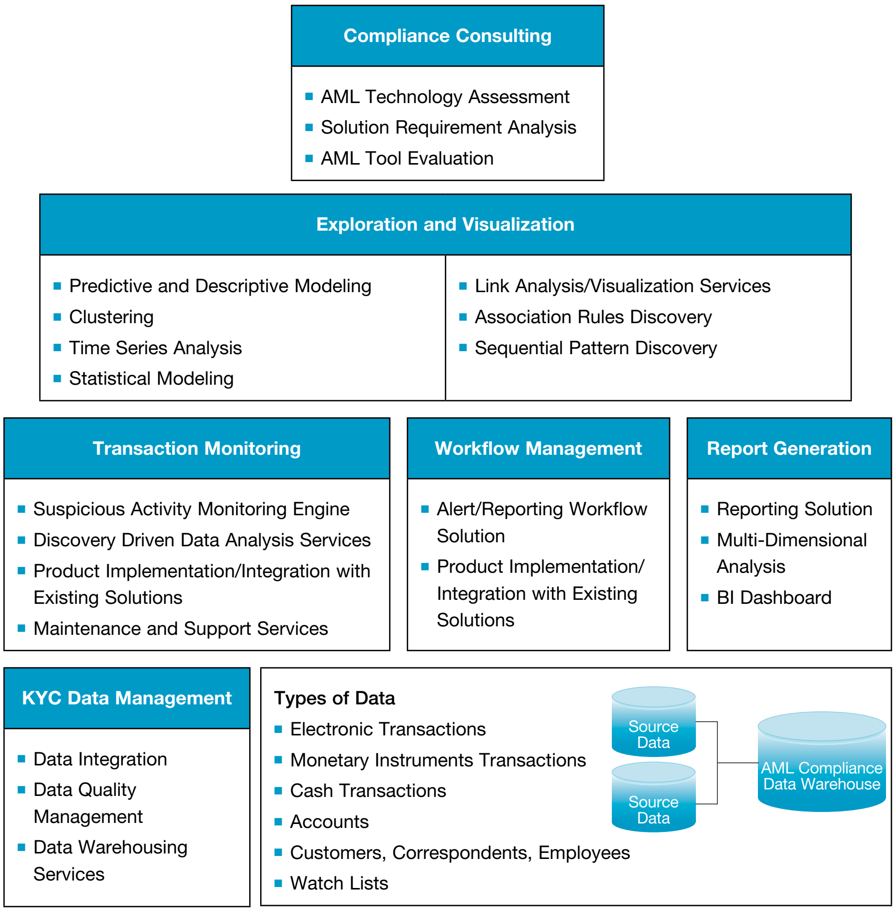
The second generation anti-money laundering solutions that are widely used today are far superior in detecting potential money laundering threats. These solutions follow an intelligent approach to anti-money laundering by way of customer risk profiling, watch list filtering, and suspicious activity reporting and monitoring. Moreover, they have the ability to analyze every customer transaction at a greater level of detail for better regulatory compliance.

5.2. Current AML Solutions Landscape for Financial Services Institutions

The financial services industry has at its disposal a wide array of technology-based tools and solutions to counter money laundering activities and meet regulatory compliance requirements. However, each financial services institution has a unique set of requirements and challenges when it comes to tackling money laundering issues. As a result, an understanding of how anti-money laundering solutions work is vitally important in choosing the appropriate path forward.

Exhibit 8 broadly explains different areas under which a financial services institution can look to understand and prevent money laundering issues.

Exhibit 8: Overview of the Anti-Money Laundering Solutions Landscape for Financial Services Institutions



Compliance Consulting
- AML Technology Assessment
- Solution Requirement Analysis
- AML Tool Evaluation

Exploration and Visualization
- Predictive and Descriptive Modeling
- Clustering
- Time Series Analysis
- Statistical Modeling
- Link Analysis/Visualization Services
- Association Rules Discovery
- Sequential Pattern Discovery

Transaction Monitoring
- Suspicious Activity Monitoring Engine
- Discovery Driven Data Analysis Services
- Product Implementation/Integration with Existing Solutions
- Maintenance and Support Services

Workflow Management
- Alert/Reporting Workflow Solution
- Product Implementation/ Integration with Existing Solutions

Report Generation
- Reporting Solution
- Multi-Dimensional Analysis
- BI Dashboard

KYC Data Management
- Data Integration
- Data Quality Management
- Data Warehousing Services

Types of Data
- Electronic Transactions
- Monetary Instruments Transactions
- Cash Transactions
- Accounts
- Customers, Correspondents, Employees
- Watch Lists

Source: Capgemini Analysis, 2011

Compliance Assessment

An assessment is the first phase financial firms should take to plan an anti-money laundering initiative. Firms need to:

- Formulate a compliance policy or evaluate an existing policy,
- Assess the risks of money laundering and create a strategy,
- Evaluate and select the right anti-money laundering tool and vendor, and
- Formulate the basic filter rules.

Financial services institutions should focus on evaluating anti-money laundering tools, assessing technology, and gathering requirement processes.

Data Exploration and Visualization

Data Exploration and Visualization includes data retrieval and analysis for specific entities; extract hidden and extended relationships; perform an evaluation of the alert management systems; and creation and modification of rules to reduce false negatives or positives.

To build a robust data exploration and visualization system, financial services institutions can leverage various options such as:

- Predictive and descriptive modeling,
- Clustering,
- Time series analysis,
- Statistical modeling,
- Link analysis and other visualization services,
- Association rules discovery, and
- Sequential pattern discovery.

Transaction Monitoring

The transaction monitoring phase involves monitoring activities across business units, services, and products; identifying suspicious activities; filtering for a given watch list, and prioritizing alerts based on risk-based scoring.

To create an effective transaction monitoring system, leading financial services institutions:

- Set up a suspicious activity monitoring engine,
- Come up with discovery-driven data analysis services, and
- Implement and integrate new products with existing solutions.

AML systems with poor algorithms run the risk of creating a large number of false positive alerts for financial entities which then need further prioritization based on risk grading. To address false positives, firms should implement solutions that operate on more sophisticated algorithms and follow an intelligent approach to screening transactions and raising alerts. Financial institutions can look at prioritizing suspicious activities by building scenarios around the customer's past alert history, past behavior, and more.

Workflow Management
This stage involves sorting, filtering, and searching alerts; automating alert assignment to queues, individuals, and groups; generating audit trails; providing supervisory approval for actions; and suppressing entity-specific alerts.

Financial services institutions can focus on building an effective workflow management program by performing alert-reporting workflow solutions in a way that ensures integration with existing solutions.

Report Generation
This stage involves automatically generating regulatory reports such as suspicious activity reports; and generating customized reports for internal and external purposes. Report generation can be automated by:

- Creating a reporting solution,
- Performing multidimensional analysis, and
- Creating a business intelligence dashboard.

Know Your Customer (KYC) Data Management
The data management and retention activities required by Know Your Customer regulations can become an arduous task for financial institutions. Addressing KYC compliance requirements can be simplified by maintaining data quality management and implementing robust data warehousing services.

A well designed KYC solution can serve as a key accelerator, helping financial institutions to respond quickly to regulatory requirements. An advanced and fully integrated KYC data management solution can help achieve increased adaptability and flexibility by supporting quick, efficient and cost effective changes to KYC rules, practices, organization and related reporting.

6 Conclusion

Various government and non-government agencies at global, regional, and national levels have come up with a specific set of regulatory guidelines and mandates for the financial services industry to control money laundering. The emergence of technology and new payment methods in the financial industry has further opened new gateways to money launderers and so increased the focus of regulators on the industry.

Financial institutions are challenged to deal with rising compliance requirements as well as to protect themselves from the legal, regulatory, and reputational risks of being associated with laundering activities.

The rising volumes of customer transactions and the increased automated interaction with customers has made compliance more complicated for these firms. Moreover, anti-money laundering is one of the largest areas of regulatory compliance spending after operational risk management[9], highlighting the importance of dealing with anti-money laundering issues at an organization level.

Firms can leverage technology by installing the best solutions available in the market according to their specific needs in order to automate most of their customary reporting activities.

[9] Datamonitor survey conducted mid-2008 with 194 IT decision makers in retail banks

References

1. Money Laundering Impacts Development, World Bank, http://www.apgml.org/issues/docs/30/WB_Impacts on development.pdf

2. *The Negative Effects of Money Laundering on Economic Development,* The Asian Development Bank, http://www.adb.org/documents/others/ogc-toolkits/anti-money-laundering/documents/money_laundering_neg_effects.pdf

3. *Money Laundering Using New Payment Methods,* FATF Report, October 2010, http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf

4. *The consequences of money laundering and financial crime,* U.S. Department of State, http://www.apgml.org/issues/docs/30/Negative Effects of ML_Economic Perspectives May 2001.pdf

5. *Financial Intelligence Units: An Overview,* International Monetary Fraud, World Bank, 2004, https://www.unodc.org/tldb/pdf/FIU_guide.pdf

6. Using Technology to Combat Financial Crime in Retail Banking, Datamonitor, December 2008

7. *Japan Financial Intelligence Center Annual Report 2009,* http://www.npa.go.jp/sosikihanzai/jafic/jaficenglishpage/jafic_2009e.pdf

8. IMOLIN, http://www.imolin.org/ accessed on September 18th, 2011

9. The Guardian, http://www.guardian.co.uk/ accessed on September 19th, 2011

10. The Economic Times, http://economictimes.indiatimes.com/The Asia/Pacific Group on Money Laundering, http://www.apgml.org/

11. The Egmont Group of Financial Intelligence Units, http://www.egmontgroup.org/ accessed on September 15th, 2011

www.capgemini.com/financialservices

About the Authors

Santosh Ejanthkar is a Lead Consultant in Capgemini's Strategic Analysis Group within the Global Financial Services Market Intelligence team. He has over seven years of experience in research and strategy consulting for investment banking, asset management, private banking, and wealth management businesses.

Leepa Mohanty is a Lead Consultant in Capgemini's Financial Services Global Business Unit. She has over 11 years of experience in credit card processing systems, transaction processing and business process management.

The authors would like to thank **Rik Boonstra**, **William Sullivan**, and **David Wilson** for their contributions to this publication.

For more information, visit **www.capgemini.com/financialservices** or e-mail **financialservices@capgemini.com**.

About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies.

Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working, the Collaborative Business Experience™.

The Group relies on its global delivery model called Rightshore®, which aims to get the right balance of the best talent from multiple locations, working as one team to create and deliver the optimum solution for clients.

Present in 40 countries, Capgemini reported 2010 global revenues of EUR 8.7 billion and employs around 112,000 people worldwide.

Capgemini's Global Financial Services Business Unit brings deep industry experience, innovative service offerings and next generation global delivery to serve the financial services industry.

With a network of 21,000 professionals serving over 900 clients worldwide, Capgemini collaborates with leading banks, insurers and capital market companies to deliver business and IT solutions and thought leadership which create tangible value.

For more information please visit **www.capgemini.com/financialservices**