Saurav Banerjee
General Manager, Quality–BFSI

Nitin Kashyap
Assistant Manager, Training–BFS

CAN THE DIGITAL REVOLUTION HELP BANKS COUNTER MONEY LAUNDERING & TERRORIST FINANCING?

WNS
Extending Your Enterprise

Executive Summary

In the 2016 movie *Money Monster*, a glitch in the trading algorithm supposedly causes the stock market to crash. But towards the end, one character says: “They’re only calling it a glitch because nobody understands how the algo works. And if nobody can understand the math, then nobody has to explain the money.”

Banks operating in a fast-changing and highly disruptive business environment today need to understand the math, money and algorithms to curb the flow of illicit money in an unevenly regulated marketplace. As criminals and terrorists thrive in this new and digitalized ecosystem, the pressure is on banks and Financial Institutions (FIs) to rev up their initiatives for Anti-money Laundering and Countering the Financing of Terrorism.

However, banks and FIs are grappling with outdated rules and systems, cumbersome compliance norms and siloed data sources. They need innovative and agile solutions that can combat Money Laundering and Terrorism Financing (TF). In this paper, we look at the specific gaps and challenges faced by banks in arriving at credible intelligence on TF, and explore the potential of digital technologies that can address the same.

Can the Digital Revolution Help Banks Counter Money Laundering & Terrorist Financing

Saurav Banerjee & Nitin Kashyap

Shadow Play

The U.S. Treasury estimates that over USD 300 Billion illicit proceeds are laundered in the U.S. financial system every year. The United Nations Office on Drugs and Crime (UNODC) estimates that less than 1 percent of these flows are seized and frozen

Introduction

USD 321 Billion. This is the amount paid as fines by global banks since 2008 for failing to comply with regulatory norms around Money Laundering (ML), market manipulation and Terrorism Financing (TF). So, what's preventing banks from taking effective measures to curb ML and TF activities? Can the same digital technologies that give criminals and terrorists the advantages of anonymity and speed help banks and Financial Institutions (FIs) improve controls and governance?

Before we delve into the possible answers to these questions, let's first look at the differences between traditional ML and TF.

ML is the concealment of illegal sources of funds, including smuggling, trafficking and fraud. TF is the collection of funds, both legal and illegal, and their channeling for the purposes of spreading terror. While ML focuses on hiding the sources of funds, TF may or may not hinge on hiding the source, but focuses more on hiding the funding activity as well as the nature of the funded activity.

The Financial Action Task Force (FATF), an international policy-making body backed by over 30 Western countries, catalogs the following ways in which terrorist organizations generate funds that eventually find their way into banking channels:

1. **Private Donations and Crowdsourcing:**

   An analysis of TF related law enforcement cases and prosecutions in the U.S. since 2001 found that approximately 33 percent of these cases involved direct financial support from individuals to terrorist networks. Social networks are also being used to coordinate fundraising campaigns. Large-scale and well-organized fundraising schemes aimed at TF may involve up to several thousand 'sponsors' and may raise significant amounts of cash.

2. **Channeling Donations Through Charitable and Non-profit Organizations:**

   A large number of traditional transnational terrorist organizations either exploit legitimate charitable and non-profit organizations, or set up sham organizations to access materials and funds.

3. **Earnings from Criminal Activities:**

   Terrorist organizations are increasingly turning to criminal activities, especially cybercrime, to raise funds. There are documented instances of counterfeiting, extortion, kidnapping and ransom, identity fraud, spurious insurance claims, and even fake or illegal e-commerce businesses being used by terrorist groups.

4. **Legitimate Commercial Enterprises:**

   Completely legal companies can be used by terror group sympathizers to route funds. There are growing instances of lone terrorists or terrorist groups using completely legal sources of money such as personal savings or online trading revenues to fund specific terror projects.

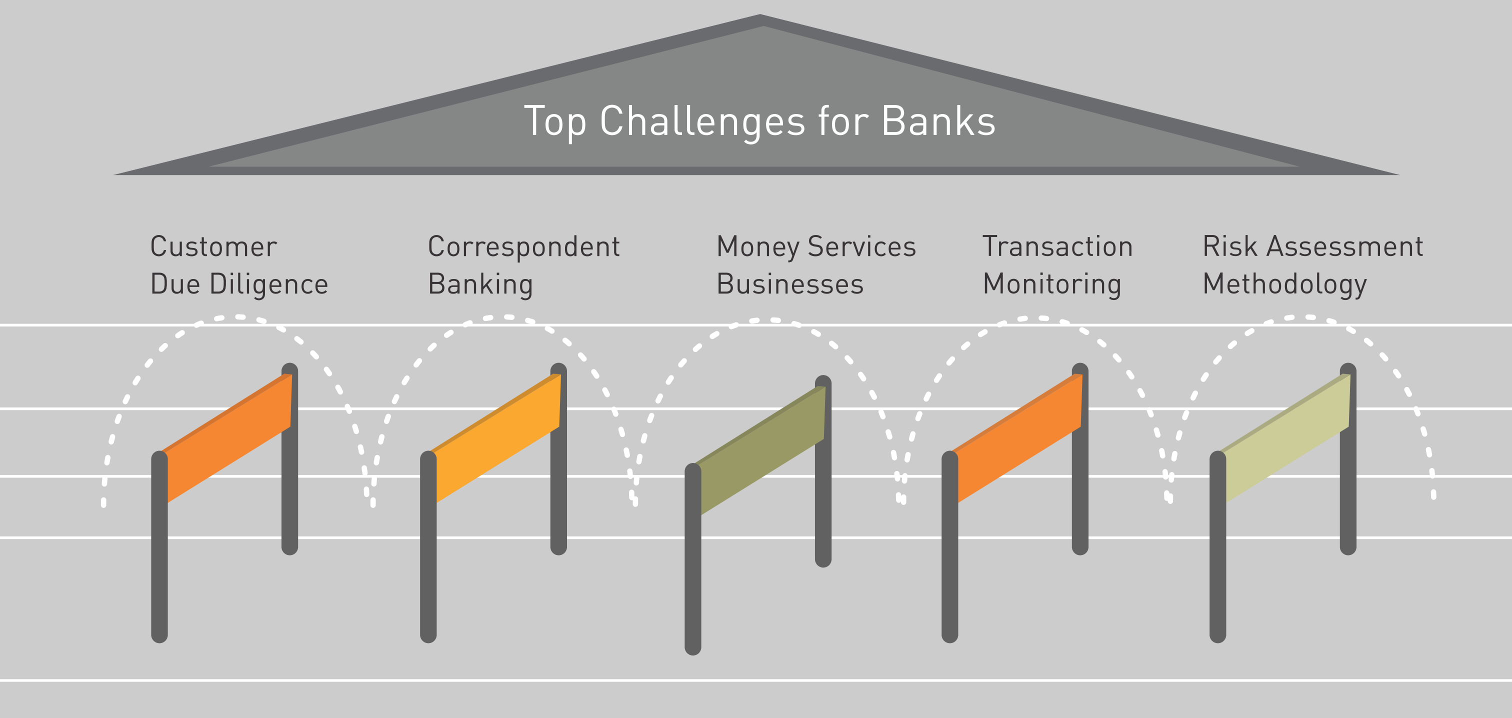
However, while there are significant differences between ML and TF, the war on terror involves elements of both Anti-money Laundering (AML) and Countering the Financing of Terrorism (CFT). The focus is on connections between individuals, between organizations, as well as between the individuals and the organizations.

Operationally, the main challenges for banks in establishing these links stem from weaknesses in the following areas:

1. **Customer Due Diligence (CDD):**
   Incomplete or missing customer profiles form the weakest link for banks as they are unable to conduct further due diligence or monitoring based on updated sanctions and black lists. For example, not having all variants of a customer's name, or mentioning only business name on transaction reports can severely hamper the credible analysis of suspicious transactions. Dealing with shell corporations, where the identities of the ultimate beneficiaries are not known, can further deter the monitoring process.

2. **Correspondent Banking:**
   Banks often execute transnational transactions through other banks or FIs that are called correspondent banks. In the backdrop of AML/CFT measures, banks are expected to perform due diligence on their correspondent banks for ML and TF risks. They are also supposed to conduct ongoing transaction monitoring on foreign correspondent bank accounts. Operationally, such due diligence is often weak or cursory. Some of the largest fines imposed on banks in recent times have been due to weak due diligence on correspondent banks in high-risk areas.

3. **Money Services Businesses (MSBs):**
   The U.S. Financial Crimes Enforcement Network (FinCEN) defines MSBs as including currency dealers, money



transmitters, issuers and redeemers of travelers' checks amongst others. MSBs can be exploited for ML and TF purposes through techniques such as structuring of transfer sizes, circumventing Know Your Customer (KYC) requirements, or exploiting negotiable monetary instruments. This poses risks for banks when these funds are integrated into regular accounts. While U.S.-based MSBs are required to register with FinCEN and comply with AML regulations, banks may have relationships with MSBs in other jurisdictions. Even within the U.S., the definition of MSBs is evolving, and often banks are unsure of the specific monitoring and compliance requirements.

4. **Transaction Monitoring:** Transaction monitoring is considered to be the backbone of AML/CFT initiatives. While most banks have Transaction Monitoring Systems (TMS) running automated checks on all transactions, their limitations are exposed when there's a huge volume of transnational and high-risk transactions. TMS raises alerts based on algorithms defined around transaction thresholds and behavioral anomalies. But as most of these algorithms are at least a decade old, they don't reflect the realities of today's ML/TF techniques. This results in a high ratio of false positives that often lead banks to review alerts in an arbitrary manner or tune the TMS to generate fewer alerts.

5. **Risk Assessment Methodology:** AML and CFT initiatives across the globe have scarce resources and slow reaction time. In 2014, the FATF issued guidelines on adopting a risk-based approach to AML and CFT measures to allow countries, competent authorities and FIs to "adopt a more flexible set of measures in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way." However, ineffective risk assessment and rating, and the lack of periodic reviews lead to failure in identifying potential ML/TF transactions.

The above operational challenges are complicated further by constantly changing regulatory requirements. A case in point is the uncertainty bred by the current U.S. administration's call to review the Dodd-Frank regulation. The Dodd-Frank Act, passed in 2010, brought in broad reforms and stricter regulations for the banking industry. It also introduced stringent AML and KYC requirements to prevent potential misuse. However, it was seen by some as 'overregulation' that badly impacted smaller businesses.

In June 2017, the Financial CHOICE Act was passed by the U.S. House of Representatives to reduce Dodd-Frank's heightened regulatory requirements. While some view the selective rollback of Dodd-Frank as a relief from burdensome financial regulations, many believe that the repeal will weaken banks' defenses against AML and TF. As the administration dwells on the repeal, in the interim, banks continue to battle ambiguity that often translates into compliance failure for some.

A Flawed System and Evolving Procedures

In February 2016, the Basel Committee on Banking Supervision released a revised set of guidelines on how banks should factor in risks concerning ML and TF while designing their overall risk management architecture. In the last year, regulators in the U.S. have given many indications of updating the framework to make it more effective. The changes include updating CDD requirements to include ultimate beneficial ownership of entities transacting with banks, and newer mandates for TMS and cybersecurity.

A recent report also mentions recommendations to FinCEN for raising the dollar thresholds for Suspicious Activity Reports (SAR). It includes greater scope for sharing information between FIs, and allowing direct sharing of raw, encrypted data with FinCEN to reduce its dependence on banks for investigations.

There's also an increase in the actions taken by financial crimes' agencies against digital entities and securities firms found to be non-compliant with AML/CFT requirements across Europe and APAC regions. While giving AML/CFT regulations more teeth globally, such cohesive actions will also serve to enhance awareness and incentivize effective controls in all stakeholder organizations.

However, even as banks recognize the need for re-engineering their AML and CFT measures to enhance efficiency and effectiveness, they are often bogged down by legacy systems, insufficient training and increasing costs. For example:

- Lack of data standardization across geographies and institutions when it comes to payments-related metadata makes it difficult to monitor real-time payments
- There is very limited coordination between banks, especially with respect to suspicious transaction reports. Increased collaboration can help track suspicious activities
- Cross-border restrictions on the transfer, storage and usage of KYC-related data are often difficult to interpret and limit the efficacy of AML-focused KYC solutions

Intel Under Pressure

The number of Suspicious Activity Reports filed by U.S. banks and FIs with FinCEN soared from over 0.6 million in 2013 to almost a million in 2016

One of the biggest brands in international banking paid fines to the tune of USD 1.2 Billion to seek deferred prosecution on charges of AML violations in 2012

A leading retail bank in a European country was fined over Euro 3 Million for failures in risk assessment and enforcement of AML/CFT rules

Global spending on AML compliance is set to grow to more than USD 8 Billion by 2017

Digital Power to Combat Terror

As calls for updating CDD requirements and sharing information between FIs is increasing, digital technologies are beginning to play a key role in tackling ML and TF. Automation, analytics and Artificial Intelligence (AI) are making huge strides by helping businesses re-design processes, mine and aggregate data, and analyze customer behavior.

New digital solutions embedded with AI and analytics have hit the market to offer banks and FIs greater visibility into transactions and ensure compliance. These solutions collect and screen customer data, and help in enhanced due diligence for onboarding customers. With predictive analytics and machine-learning capability, there are platforms and solutions that can enable banks and FIs to monitor global transactions with ease.

Digital technologies can help banks and FIs get richer, real-time, actionable and intelligent insights to manage ML and TF risks. Workflow tools can make the reporting mechanism simpler and the audit trail clearer. Web technologies can offer simpler screening processes and drastically reduce costs. By connecting the data from multiple systems and sources, digital technologies can help banks and FIs craft strategies to manage risks and improve governance. These technologies not only reduce costs and simplify the AML/CFT processes, they can help banks and FIs increase revenue and ensure the protection and privacy of data.

Let's now take a brief look at the remedy offered by digital solutions specifically in KYC and TM.

Know Your Customer

Covering the processes of customer onboarding, monitoring and screening, digital solutions enable a single point access to various internal and external sources of information, including Customer Relationship Management (CRM) databases. Automated screening for sanctions' violations, status of Politically Exposed Person (PEP), adverse media mentions, as well as beneficial ownership information across all sources enhances the efficiency of customer onboarding significantly. Proprietary databases of corporate registries and individuals from across geographies offer greater advantage in discovery and verification of beneficial ownerships.

Some solutions offer data quality checks that allow banks to standardize data formats, correct errors in names, as well as deduplicate customer records across sources. This also enables establishing links and relationships among customers and businesses with greater accuracy. Visualization tools allow compliance officers to share complex relationship networks with ease across different stakeholders.

Transaction Monitoring

TM solutions leverage advanced analytics and AI extensively to monitor, assign risk ratings, raise alerts, manage alert workflows as well as report suspicious transactions. Banks can choose to automate real-time monitoring, or perform monitoring in the batch processing mode.

Most solutions come with pre-defined domain-specific detection algorithms and scenarios, and offer customization capabilities to modify screening based on customer or transaction risk assessments. This is a critical capability that can help traditional transaction management overcome the shortcoming of delayed scenario building for newer searches.

Solutions leveraging machine-learning technology offer self-learning algorithms and allow for greater sophistication in the detection of suspicious transactions. Including the capability to monitor affiliated MSB and broker activities in the same platform can significantly enhance the effectiveness of TM. Inbuilt workflow, visualization and audit tools ensure that alerts, reporting and audit trails are efficiently managed.

The Loopholes to Fix

For criminals and terrorists, unregulated online payment gateways are an avenue to funnel money for illegal or terrorist activities. Digital and cryptocurrencies are other channels for anonymous dealings. For example, all transactions on Silk Road — the now defunct online market for illegal drugs — were done using bitcoins. Buyers and sellers could anonymously access the website, a part of the dark web, without the risk of being monitored. The Federal Bureau of Investigation cracked down on the website in October 2013.

As digital payment networks are transnational, laws of one country do not apply to another. Thus, a less regulated environment provides criminals and terrorists the scope to operate across the world. In 2017, the WannaCry ransomware attack affected over 200,000 computers across 150 countries. Hackers behind the attack held computers hostage by encrypting data and demanding ransom payable in bitcoins. Ransomware attacks numbered 483,800 in 2016 alone and hackers continue to use advanced digital tools to launch cyber attacks.

However, equipped with the sophisticated capabilities of AI and analytics, banks can bring in greater scrutiny by factoring scenarios that signal potential suspicious activities into their TM strategies. Scenarios such as dormant accounts receiving sporadic deposits or frequent wire transfers in small amounts to avoid identification should trigger alerts for further scrutiny. Here's a small, but not exhaustive, list of scenarios that banks can watch out for:

- An account in which several people have the authority to sign, but don't seem to have any family or business relationship
- Deposits for a business entity in which a combination of monetary instruments are used that do not match the normal activities associated with such a business (for example, deposits that include a mix of business, payroll and social security checks)
- Large cash deposits or withdrawals made from a business account not normally associated with cash transactions
- Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries

Tracking these anomalies can help banks and FIs monitor some of the more recent techniques involved in the flow of illicit money.

Coming up to Speed

KYC compliance requires manual access and review of relevant information across different sources

PwC estimates that out of 100, more than 90 Transaction Monitoring alerts are ignored due to scarce resources. Of the remaining, 8 alerts are false positives

Conclusion

The niche and growing Regulatory Technology (RegTech) industry hopes for greater dialogue among regulators, FIs and RegTech companies. Open discussions on regulatory architecture, data formats and compliance related challenges can help speed up the deployment of digital technologies and innovations.

So far, CFT and AML efforts have been operating as silo functions across banks and FIs. Data-sharing procedures were vague. The banking industry now needs to move towards adopting an integrated risk assessment approach to allow for a more holistic and streamlined understanding of AML and CFT risks. Regulators need to address the lack of standardization and the need for far greater collaboration among FIs. These measures will bring AML and CFT measures under one roof, and enable the banking industry to fight new threats in ML and TF. It will provide greater transparency and allow FIs and regulators to set more clear guidelines.

Innovative digital solutions can address the gaps in banking operations and ease the process for an industry struggling to tamp down rising costs and stretching its resources further. Analytics and AI are just a couple of such elements that will transform and benefit AML and CFT measures. Partnering with third-party players with proven expertise in analytics and AI can also help banks counter the menace of ML and TF.

References

i. http://www.worldbank.org/
ii. http://www.fatf-gafi.org/
iii. https://www.treasury.gov/
iv. https://www.unodc.org/
v. https://www.iif.com/
vi. https://www.bloomberg.com
vii. http://fingfx.thomsonreuters.com/
viii. http://www.bis.org/
ix. https://www.pwc.com/
x. http://www.coindesk.com/
xi. https://www.wilmerhale.com/
xii. https://www.theclearinghouse.org/
xiii. http://thelaundromat.kwm.com/
xiv. http://www.al-monitor.com/pulse/home.html
xv. https://www.wilmerhale.com/

WNS (Holdings) Limited (NYSE: WNS) is a leading global Business Process Management (BPM) company. WNS offers business value to 200+ global clients by combining operational excellence with deep domain expertise in key industry verticals, including banking and financial services, healthcare, insurance, manufacturing, media and entertainment, consulting and professional services, retail & consumer packaged goods, telecom and diversified businesses, shipping and logistics, travel and leisure, and utilities. WNS delivers an entire spectrum of business process management services such as customer care, finance and accounting, human resource solutions, research and analytics, technology solutions, and industry-specific back-office and front-office processes. WNS has delivery centers world-wide, including China, Costa Rica, India, the Philippines, Poland, Romania, South Africa, Sri Lanka, UK and US.

To know more, write to us at
marketing@wns.com or visit us at www.wns.com

WNS
Extending Your Enterprise