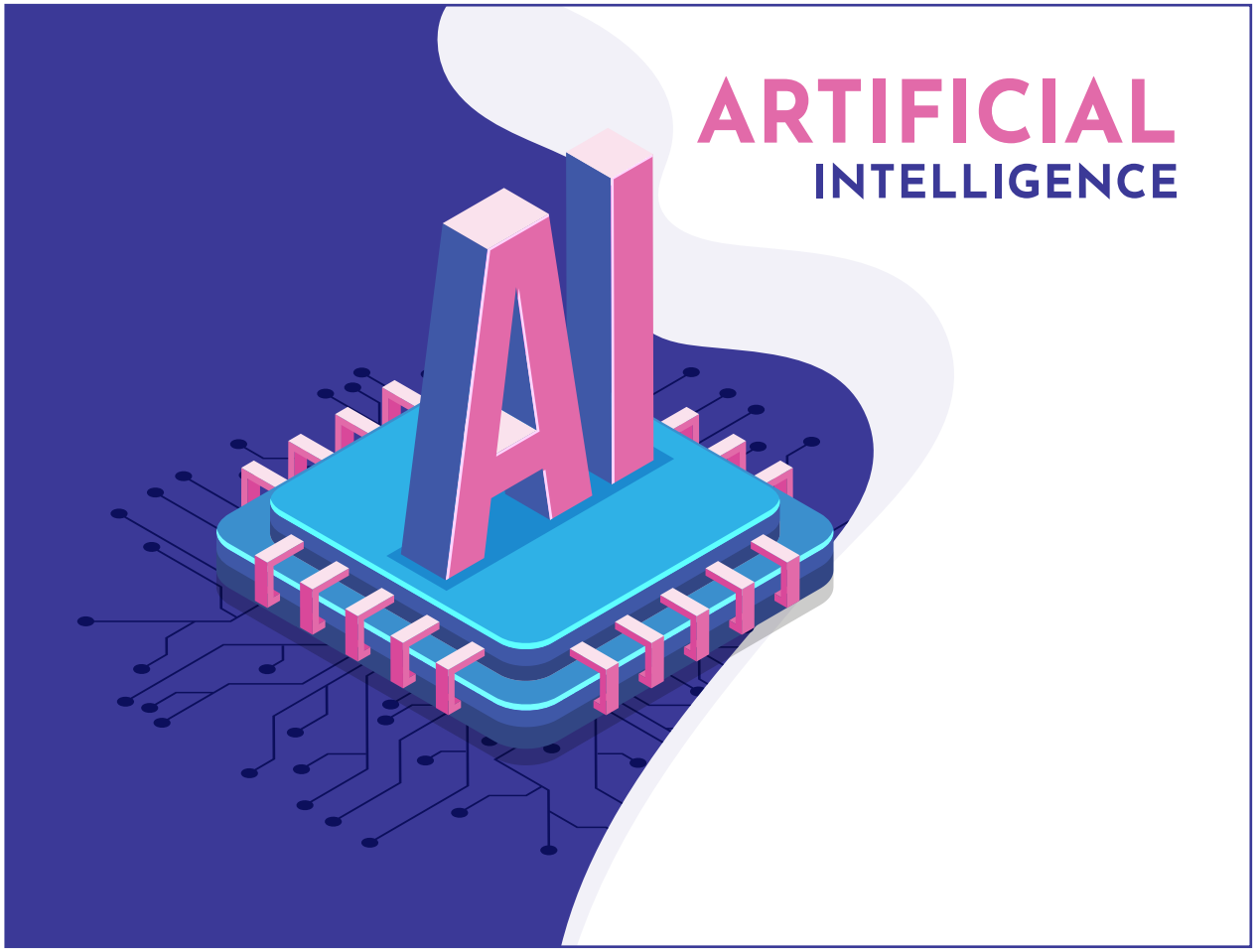

AI AND AML

Financial crime and, in particular, Money Laundering is a complex issue for financial institutions. All financial services organizations must operate appropriate processes and controls to deter criminals from using their products and services to facilitate Money Laundering and terrorist financing activities. Unfortunately, the burden of running Anti Money Laundering (AML) processes, in terms of resources and costs, the increase in transactional volumes and the high level of false Money Laundering alerts continues to grow and, as these challenges increase, so do the regulatory fines. US regulators alone have handed out fines for AML-related compliance failings, mainly related to sanction breaches, to over $17 billion since 2009.

The people behind Money Laundering are determined, sophisticated criminals who fund global terrorism, human trafficking, and narcotics distribution.

The methods used to launder proceeds of criminal and financial illicit activities are in constant evolution. Banks and financial institutions must work tirelessly and continuously with international organizations, governments, law enforcement agencies, regulators and industry peers to identify new threats of Money Laundering and close off channels within the financial system that criminals may use. Unfortunately the techniques used by criminals continue to

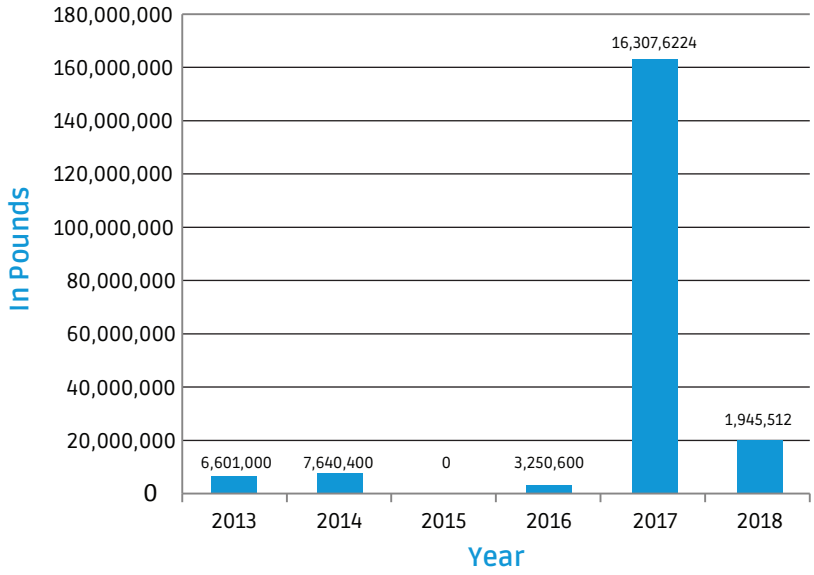

Figure 1: FCA AML Related Fines

develop and have become ever more sophisticated. Professional Money Launderings will always adapt, probing for weaknesses in financial systems that can be exploited.

So, what are the latest threats faced by the industry in 2018? What measures are being deployed to address these threats and how do organizations develop a partnership with the FinTech and RegTech community to support innovation in financial services?

Money Laundering is an illegal activity performed outside of the normal range of economic and financial statistics. The United Nations Office on Drugs and Crime (UNODC) estimates that the amount of money laundered globally in one year is 2 - 5% of global GDP, or $800 billion - $2 trillion in current US dollars. As the key objective of Money Laundering is to get the illegal funds back to the individuals who generated them, launderers usually prefer to move funds through stable financial systems.

Money Laundering activity is typically concentrated geographically according to the stage the laundered funds have reached. At the placement stage, the funds are usually processed close to the under lying activity; in the layering phase, the launderer might choose an offshore financial or regional business center. Finally, at the integration phase, launderers might choose to invest laundered funds in other locations to enhance investment opportunities.

Money Laundering - The Threats

The Financial Action Task Force (FATF) identifies three key methods by which criminals and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. These include the use of the financial system; the physical movement of money and of goods through the trade system. All three methods directly and indirectly involve banking systems.

Money launderers also use a wide variety of tools and techniques. Among the most significant and common are:

Trade-based Money Laundering

This is the process of disguising the proceeds of crime and moving

THE UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC) ESTIMATES THAT THE AMOUNT OF MONEY LAUNDERED GLOBALLY IN ONE YEAR IS 2 - 5% OF GLOBAL GDP, OR $800 BILLION - $2 TRILLION IN CURRENT US DOLLARS

value through the use of trade transactions in an attempt to legitimise their illicit origin.

Account Settlement Mechanisms

Money launderers can facilitate the settlement of accounts between multiple organized crime groups.

Underground Banking and Alternative Banking Platforms

This mechanism is used with the goal of bypassing the regulated financial sector and creating a parallel system of moving and keeping records of transactions and accountancy.

Money Value Transfer Services (MVTS) Providers

Complicit insiders (e.g. bankers) act as potential accomplices to help launder illicit proceeds and participate in the placement stage of the Money Laundering process

Financial Institutions

The use of the international financial system has been instrumental in facilitating large-scale Money Laundering schemes. All of the complex layering schemes involve moving significant volumes of funds through various bank accounts in different jurisdictions opened on behalf of shell companies.

Legal and Professional Services

In order to place greater distance between their criminal activity and the movement of funds, some organized criminal gangs use the services of third-party Money Launderings, including professional gatekeepers, such as attorneys, accountants and company service providers.

Payment Processing Companies

Payment processing companies provide services to merchants and other business entities, such as credit card processing or payroll processing services. In certain circumstances, payment processing companies essentially act as "flow-through" accounts.

How do banks comply with applicable Anti Money Laundering (AML) laws and regulations in the juristictions in which they operate?

First and foremost, banks need to meet the standards set by regulators and adhere to local legislative and regulatory requirements in all juristictions in which they operate. They must maintain a strong AML goverance model with defined responsibilities and accoutabilities.

Described below are key elements that an AML program must have in place to prove to regulators that proper controls are in place that can protect the organization completely.

A Risk Appetite that Supports the Organization's Strategic Risk Objectives

Risk appetite is the residual risk that banks are prepared to accept as a consequence of doing business, This will provide the foundation for the bank's AML policy. Its AML risk must ensure controls are appropriate to the level of risk and must be designed to prevent or identifty non compliance.

A Risk-based Approach

Many banks take a risk-based approach of dealing with their customers and assign resources and controls that are appropriate to the inherent AML risk. This is fundemental to the prevention of Money Laundering and ensures that resources are adequately applied to those areas that the bank has deemed to be most at risk. A typical example would the application of risk categorization to all customers where a high, medium or low risk is applied to customers determined by a documented risk methodology.

Customer Due diligence

Knowing Your Customer (KYC) is fundamental to AML. The term encompasses knowledge, understanding and information obtained about a customer throughout the lifecycle of the relationship, and this will include transactions and the use of products. Other important factors are the source of a customer's funds and wealth, the nature of the relationship, customer verification and beneficial owners and high risk identifiers.

Politically Exposed Persons (PEPS)

A PEP is an individual who holds a prominent public function. Identification of PEPs are required to manage the risk associated with persons who may abuse their position or influence for their own personal benefit. This is especially pertinent in jurisdictions that are economically or politically unstable or tainted by high levels of private or public corruption and criminal activity.

Transaction Monitoring

Banks will actively monitor transactions and customer activity to ensure that they are consistent with their knowledge of the purpose of the transaction, the customer, their business and risk profile. Monitoring customer activity will help identify unusual behaviour that cannot be reasonably explained and may be indicative of Money Laundering. Unusual activity can include abnormal size of transactions, high volumes of cash credits and frequent unexplained withdrawals. Ongoing

monitoring will also include keeping customer information up to date and reviewing activity and transactions during the relationship.

Suspicious Activity Reporting (SAR)

Any suspicious activity must be documented and communicated. A nominated officer is responsible for receiving and investigating internal suspicious reports to determine whether a Suspicious Activity Report is submitted to the relevant authorities.

Sanctions

Banks undertake real time screening of transactions against a relevant sanctions list and restricted countries. Documentation and investigation of all potential matches is performed, and reports are submitted for any confirmed hits.

Other AML practices include:

- A Money Laundering Reporting Officer (MLRO), who is the focus for the firm's AML activity
- Assurance to test the operational effectiveness of AML programs
- Record keeping, retrieval and sharing of information in keeping with local regulatory requirements
- Periodic and timely tracking, collection and analysis of Management Information over AML
- Training to ensure all staff maintain awareness of AML policies

Emerging Money Laundering Threats

With the recent rapid growth of digital technologies, banks are now confronted with evermore sophisticated Money Laundering threats. Digital mobile platforms, new payment methods and techniques, cryptocurrencies, e-wallets, Distributed Ledger Technologies and instant payments are placing increasing demands on financial crime control processes

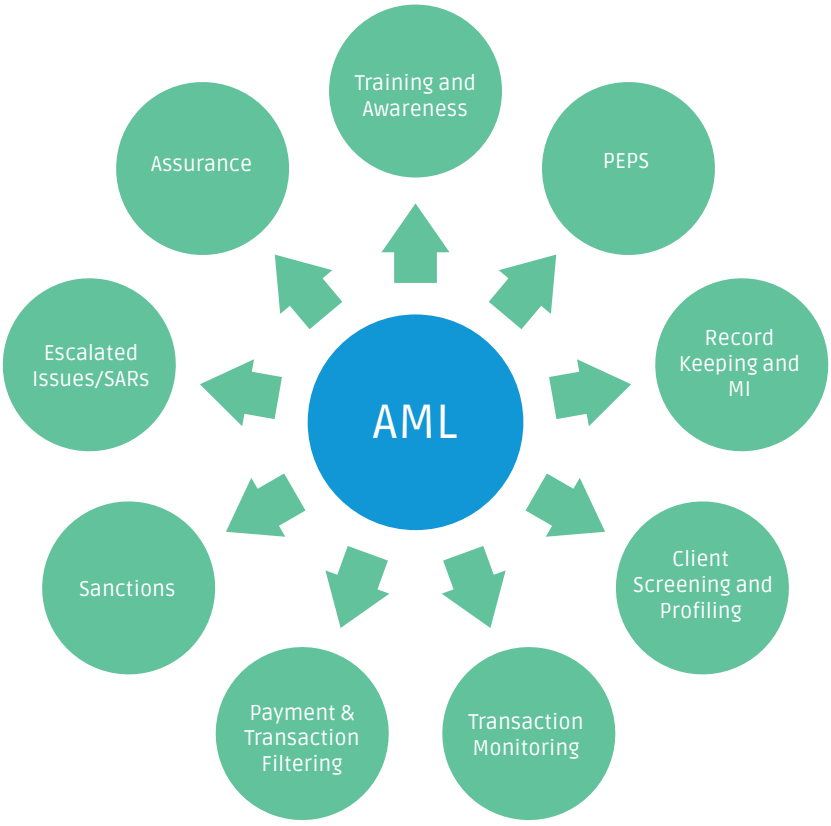

Figure 2: AML Data Sources

MANY AML AND SANCTIONS SCREENING PROCESSES HAVE BEEN DEVELOPED ON LEGACY SYSTEMS THAT ARE UNABLE TO FUNCTION, OR ARE NOT SCALABLE AND UNABLE TO OPERATE IN THE NEW REAL-TIME PAYMENTS REALITY

and real-time screening being conducted by banks and financial institutions. The variety of ways that criminals may acquire, move, disguise and dispose or otherwise launder the proceeds of crime means that the threat is unabating. In keeping with the digital era and economy, Money Laundering has evolved to involve the following:

Virtual Currencies and Blockchain

Convertible virtual currencies that can be exchanged for real money are potentially vulnerable to Money Laundering abuse. They may allow greater anonymity than traditional non-cash payment methods. They are generally characterized by non-face-to-face customer relationships, and may permit anonymous funding. They can also permit anonymous transfers if participants are not adequately identified. Some virtual currencies, like cryptocurrency, store all transactions on a blockchain which only records the transactions, not the identities, of the users. It is possible to associate Internet Protocol (IP) addresses with cryptocurrency transactions; however, routers can be used to hide a user's IP address, granting total anonymity.

New Payment Products and Services

Electronic, online and new payment methods pose a vulnerability as the use of these systems grows. Payment systems can be accessed globally and used to transfer funds quickly. Online payment systems are anonymous by design, making them attractive to criminals, particularly when the payment system is based in a jurisdiction with a weak AML regime.

Internet Payment Services

Internet-based payment services provide mechanisms for customers to access prefunded accounts. These are then used to transfer the electronic money to other individuals or businesses which also hold accounts with the same provider.

New Financial Crime Technology Capabilities in the Digital Era

So what AML systems do banks deploy and what level of automation exists to monitor and detect Money Laundering? Banks have become more aware of the financial crime threats they face and have developed responses more effectively than ever before. Furthermore, financial systems are continuously being strengthened as the partnership between banks, regulators and law enforcement agencies develops.

Customized in-house development of AML solutions allows an organization to tailor software to meet their needs. On the downside, ever-changing AML regulations can result in significant costs to an organization to meet compliance requirements. In addition, many AML and sanctions screening

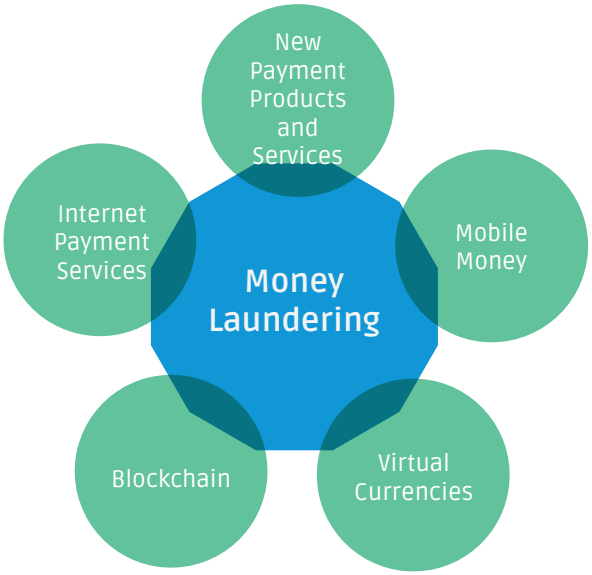

Figure3: Emerging Risks and Current Trends

IT IS POSSIBLE TO ASSOCIATE INTERNET PROTOCOL (IP) ADDRESSES WITH CRYPTOCURRENCY TRANSACTIONS; HOWEVER, ROUTERS CAN BE USED TO HIDE A USER'S IP ADDRESS, GRANTING TOTAL ANONYMITY.

processes have been developed on legacy systems that are unable to function, or are not scalable and unable to operate in the new real-time payments reality.

The acquisition of a commercial-off-the shelf software package is an alternative to in-house development. By adapting a pre-built system for AML, banks can maximize all the benefits of a custom developed system without the time and expense. The downside is that the package may not addresses all customer needs resulting in some customization to get the software to meet their initial needs. Technology-based innovations are starting to radically change the financial services industry. The identification and dismantling of Money Laundrings requires intelligence gathering and investigation of laundering activities. Dismantling of Money Launderings can impact their operations and can be an effective intervention strategy against criminal targets.

AI and Machine Learning

AI and Machine Learning are rapidly developing to become a major disruptor within the Regtech area. AML platforms with advanced technical capabilities are eliminating the complexity of managing siloed systems and multiple vendors. Machine Learning and advanced automation can replace manually intensive parts of the AML process with insights that are specific to Money Laundering. This allows banks to separate meaningful high value risk alerts from spurious data, ensuring that manual investigation resources are applied using a risk-based approach. AI can take in disconnected risk signs across payment platforms, geographies, depositors and payees, and connect the signals in meaningful ways.

Other benefits include:

- The investigations of suspicious transactions, which can be highly time-consuming, and often, due to overly-defensive mechanisms, fall victim to unsuccessful outcomes.
- The monitoring of intricate patterns via Machine Learning, reporting serious as opposed to false positive transactions for escalation and investigation by AML officers.
- Machine Learning being able to examine granular data to detect and uncover incompatible relationships, and, subsequently, complicated patterns of money laundering.
- Reducing the incidence of false positive transaction monitoring hits, allowing compliance teams to focus on the genuine ones.

As digital technologies improve and diversify, so do the threats facing banks. F inancial institutions should consider fighting financial crime with new and innovative technology in alignment with their historical approach. To ensure continued compliance, financial institutions need to embrace new technologies and integrate intelligent automation into their compliance programs.

AI CAN TAKE IN DISCONNECTED RISK SIGNS ACROSS PAYMENT PLATFORMS, GEOGRAPHIES, DEPOSITORS AND PAYEES, AND CONNECT THE SIGNALS IN MEANINGFUL WAYS

Andrew Dobbs
Solution Architect
TCS Financial Solutions (TCS BaNCS)