UGR Consulting

AML Challenges and Technology Solutions

Authored by:
Hourad Afsar, CAMS
Diana Barrero Zalles, Yale MBA

April 2018

Table of Contents

I Introduction: Evolution of US AML

Money laundering is the process of concealing the origins and ownership of money generated through criminal activity[a]. The practice of disguising income derived from illicit activities can be traced back to a few centuries ago, while the criminalization of the actual or attempted laundering of proceeds of crime is only recent. In today's globalized world, proceeds can be wired from one financial institution to another instantaneously, opening avenues for illegitimate activities.

As the banking system develops in complexity and sophistication, so does criminal activity and the AML systems in place to eradicate it.[1] With the digital revolution and the proliferation of electronic transfer systems, evolving criminal methodologies are an increasing threat to the financial services industry. [b] The Financial Action Task Force (FATF) estimates that these crimes represent 2-3% of gross world product, or $1.38-$3.45 trillion per year.[2]

AML efforts are becoming increasingly global due to the nature of cross-border activities with evolving tools to detect crime and unprecedented levels of regulation to control it. [3] The US has strived to become a frontrunner against money laundering and terrorist financing initiatives,[4] with the Bank Secrecy Act (BSA) established in 1970 and the USA Patriot Act in 2001.[5] Today's AML regulatory environment includes widespread laws that have extended to reporting for cross-border electronic funds transmittals since 2004,[c] ample guidance, and enforcement at the federal and state level.

Most recently, the Financial Crimes Enforcement Network (FinCEN),[d] the US Treasury Department bureau designated to oversee BSA compliance, added a fifth element to the existing pillars of effective AML compliance that are:
1. Development of written internal policies, procedures and controls
2. Designation of an AML compliance officer
3. Ongoing AML employee training
4. Independent testing of the AML Program[6]

---

[a] As defined by FinCEN, money laundering "involves three steps: placement, layering and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the 'dirty money' appears 'clean.'"

[b] While the global scope of money laundering and terrorist financing is extremely difficult to measure in the absence of concrete quantitative data, the Basel AML Index identifies indicators that, without confirming the existence of illicit financing, point to risks that increase the likelihood of these activities in 149 countries. A heightened risk of money laundering is reflected by a given country's lack of public transparency, high levels of perceived corruption, shortfalls in AML/CFT frameworks, poor financial standards and transparency, and weak political rights and rule of law.

[c] Among the most recent US AML laws, the Intelligence Reform & Terrorism Prevention Act of 2004 further amended the Bank Secrecy Act to regulate the reporting of cross-border electronic fund transfers, with the aim of combating money laundering and terrorist financing.

[d] FinCEN's mission is to "safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activity." It is bound by the USA Patriot Act to require US financial institutions to abide by established pillars of effective AML compliance.

The Customer Due Diligence (CDD) rule, effective as of May 11, 2018, requires covered financial institutions[e] to enhance their CDD procedures by collecting and verifying information about the individuals (Beneficial Owners[f]) who control or, directly and indirectly, own 25% or more of the equity interests of a legal entity customer. This amendment to the BSA regulations improves established procedures for US financial institutions.[7]

Consequently, financial institutions have to adapt the CDD rule seamlessly, across bank operations that encompass both US and often international operations. This calls for a better cooperation through a robust AML program.[8] Meanwhile, regulators are striving to enact the right infrastructure and systems to detect and deter illegal transactions, making compliance often burdensome for financial institutions and the environment strongly intense.

The emergence of regtech solutions brings new avenues to facilitate compliance and overall AML efficiencies.[9] The vast array of technological tools that have been developed offer promising options to improve AML processes; the right technologies can prevent many system vulnerabilities.[10] This is a work in progress, with solutions that have been implemented to different degrees across organizations. Even regulators have not yet fully embraced tech solutions so as to endorse their adoption across the board. In light of the current regulatory environment, this paper discusses these technological advances for today's AML challenges: customer screening, transaction monitoring, and cryptocurrencies, outlining areas where specific technologies are most effective. Finally, it will reflect on the role of subject matter expertise (SME) to support companies implementing these programs in light of the most pressing AML issues.

2 Customer Screening

2.1 Customer Screening Challenges

2.1.1 Complete Customer View

Financial Institutions should aim toward a 360-degree view of customers, which reveals the entire picture of both individuals and legal entities as users of financial services.[11] Yet they often store user data on dispersed systems and databases. This can lead to opaque and disjointed views of customers, where multiple profiles can be generated for a single client across jurisdictions and branches of a bank (retail banking, mortgage departments, commercial banking, credit card divisions, etc.).

Most banks cannot coalesce accounts with certain disparities, such as name or address variations, into a unique profile for a given customer. This represents information gaps in verifying customer identities, their relationships with business partners, the source of their assets, and how they use those assets: material that is essential in determining risk of money

[e] Institutions include banks, money services businesses, broker-dealers, mutual funds, and commodities brokers, with certain exceptions by type of institution.

[f] The CDD Rule defines beneficial owners as individuals who, directly or indirectly, own a minimum of 25% equity interest of a legal entity customer of a financial institution (ownership test), or individuals with "significant responsibility to control, manage, or direct a legal entity customer" such as CEOs, executive officers, senior managers, Presidents (control test).

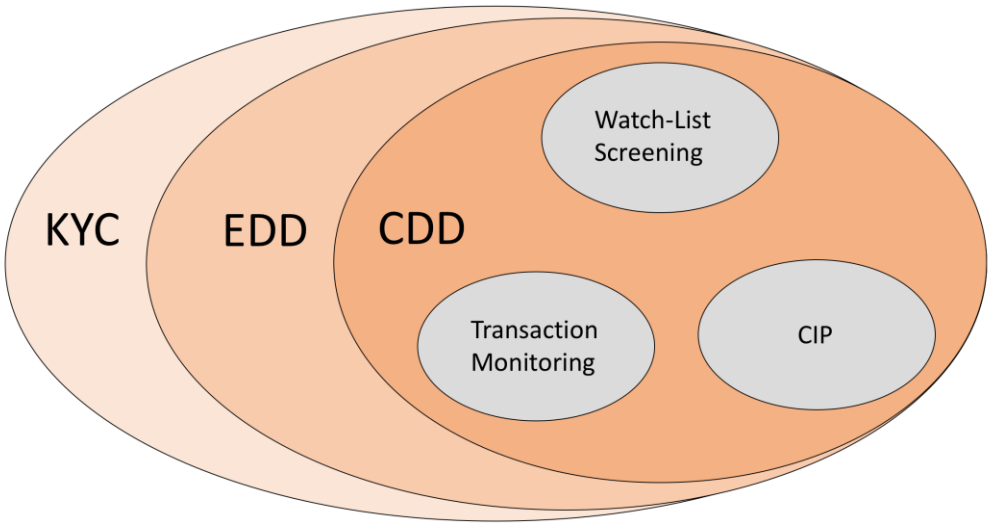
laundering. The inability to fully examine the transactions, networks, and locations where a client conducts business activities is reflected in different risk scores assigned to separate accounts pertaining to a single individual or legal entity. A lack of clarity on whom a financial institution is doing business with diminishes overall confidence on the reliability of these risk profiles.

Moreover, inaccurate or forged user identities can be the source of undetected irregular activities. Because illegal activity largely unfolds in anonymity, hackers and criminals can operate more freely under false identities or duplicate profiles of existing individuals, as their own may not pass security screenings. Hence the risk of identity theft may go unnoticed in the absence of a holistic customer view across business lines and legal entities. The 2017 Equifax data breach points to existing vulnerabilities in internal systems that can seriously compromise the safety of customer data. According to Experian, universal customer profiles can go beyond the 360-degree view and combine data from various sources including conventional identity collection, device usage, online behavior, biometrics, transaction history, and user interactions across businesses and industries, allowing companies to better identify legitimate customers from fraudsters, ultimately building trust.[12]

2.1.2 High Risk Customers & Politically Exposed Persons (PEPs)

Effective customer screening depends on identifying precarious individuals and the entities they control. KYC principles require screening prospective and existing customers to clear regulatory requirements, ensure valid identification, and determine the likelihood of financial crime. This entails detailed vigilance upon initial client onboarding and ongoing examinations. Yet incomplete identification data can undermine the quality of due diligence for high risk accounts.

KYC Program Overlay



Source: "Integrating KYC Into the Digital Age and Enterprise-wide Transformation Strategy," ACAMS Webinar, March 7, 2017, https://www.acams.org/webinar-kyc-digital-age-enterprise-wide-transformation-strategy/.

Even if banks had perfect customer information, identifying and monitoring high-risk accounts remains a challenging task due to the various different screening tools to refer to.[13] Enhanced Due Diligence (EDD) requires detailed due diligence on risky customers, as well as their associated parties, beneficiaries, and controllers. While financial institutions can and do pinpoint these high-risk customers from their existing customer base through a range of tactics, these aren't necessarily consolidated and are difficult to optimize across an organization.

From looking up the individuals behind higher risk activities to reviewing subjects of past suspicious activity investigations, there is a plethora of internal, public, and proprietary data to sort through. Some strategies entail checking internal records for involvement in large volume transactions, precarious geographical locations, and high-risk industries such as those identified by the North American Industry Classification System (NAICS). Others conduct specific keyword searches across customer databases and transaction details (check cashier, casa de cambio, jewelry, car, wire, cash, etc.). Others still involve media checks to uncover adverse news coverage on a given client, or querying account officers and customers directly.

Watch-list screening specifically poses the challenge of utilizing and aligning with a wide range of available lists; such lists cover sanctioned persons and entities (ex: SDNs), politically exposed persons (PEPs), subjects of negative media stories, etc.[g] Screening requires navigating multiple list providers.[h] There are also additional compliance requirements for specific categories of individuals such as PEPs[i] and non-resident aliens (NRAs).[j] For PEPs in particular, the influence they can lever due to their prominent public charge could facilitate involvement in risky activity such as bribery and corruption, and thus due diligence must be more stringent. For banking institutions, failing to identify these individuals and adhere to proper screenings can lead to penalties for non-compliance, if not the reputational and financial costs of enabling illegal activity.

Tech Needs:

- Create a 360-degree customer view by consolidating customer information in a standardized way. This entails linking data sources and managing big data to eliminate incomplete, inaccurate, or conflicting records. Information sharing can be key to understanding clients, their relationships, and their assets.

[g] Various vendors, including credit bureaus, offer lists and databases with sanctioned individuals and entities, PEPs, and subjects of negative media. Some lists can be accessed by Internet/ad hoc searches, available to either individuals or to institutional accounts.

[h] Providers include OFAC sanctions lists, US trade-based programs, FBI's Terrorist Screening Database (TSDB), UN Terrorist List, World Watch, proprietary databases, and credit bureaus.

[i] Section 312 of the USA PATRIOT Act (formally known as "Special Due Diligence for Correspondent Accounts and Private Banking Accounts") outlines specific due diligence and enhanced due diligence required for PEP customers, identified as non-U.S. persons and senior foreign political figures. https://www.fincen.gov/fact-sheet-section-312-usa-patriot-act-final-regulation-and-notice-proposed-rulemaking

[j] NRAs indicate heightened money laundering risks originating from challenges in verifying their identities, sources of wealth, and relationships; frequency of international transactions; potential residency in high-risk jurisdictions with lax AML regulatory structures; and increased likelihood of being PEPs. NRAs are also more likely to be victims of human trafficking and migrant smuggling. https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_085.htm

- Safeguard digital identities and validate the authenticity of clients, while implementing effective cybersecurity programs.[14] For example, FINRA published a cybersecurity checklist for small firms, and several vendors offer cybersecurity packages for institutions to secure the storage of personal details.
- Identify high-risk individuals among existing and new clients by optimizing strategic screening and information sharing.

2.2 Customer Screening Solutions

2.2.1 Consolidating and Screening Customer Profiles

Automation can consolidate redundant profiles to enable a 360-degree view of customers, combining structured and unstructured data to ensure accuracy and completion. Tracing data lineage to primary sources enables reconciliation and efficient updates, while validating its authenticity. Moreover, artificial intelligence can transliterate across alphabets to combine and standardize different variations of account names and addresses, in order to resolve entities on a global level.[k] These tools can sort through massive amounts of data on occupation, nature of business activities, and commercial relationships including accounts with related parties, purpose of transactions or accounts in question, and adverse media coverage.[l] As a result, better data management enhances the quality of CDD and EDD.

Automation enables complete access to the information necessary for monitoring and investigation. It enables tools for customer segmentation on individual, household, and organizational levels. Outputs can produce customized lists of clients, such as those who have been previously investigated and cleared. In addition, 360 customer views can be cross-referenced with high risk customer screenings. If a group of related profiles shows a pattern of false positives, or when a series of similar false positives portray a similar customer trait, this may indicate a red flag. Further exploration on the reasons why a given trait (ex: region) is producing particular alerts can influence how risk scores are weighed.

Particularly for watch-list screenings, models with filtering techniques can pinpoint high-risk customers, red flagging instances warranting further investigation. There are a number of vendors providing turn-key tools with ongoing updates based on sophisticated data analytics and data mining linked to multiple sanctions lists. Generally, “fuzzy logic” matching systems between customer lists and watch-list data allow for name variations and determine a score for the closeness of a given match. False “hits” can be reduced by tailoring the system to ignore matches with scores below a certain threshold, or with discrepancies in important information such as date of birth, country of origin, etc. Finally, false positives that don’t go into alerts can be recorded for future review, white list management, and audit.[15]

---

[k] A customer going by the first name “Michael” in the United States may use “Mikhail” in Russia or “Muhammad” in Egypt. An address can be recorded as 42 Oakdale Street and 42 Oak Dale Rd. for different accounts. Artificial intelligence can coalesce these records.

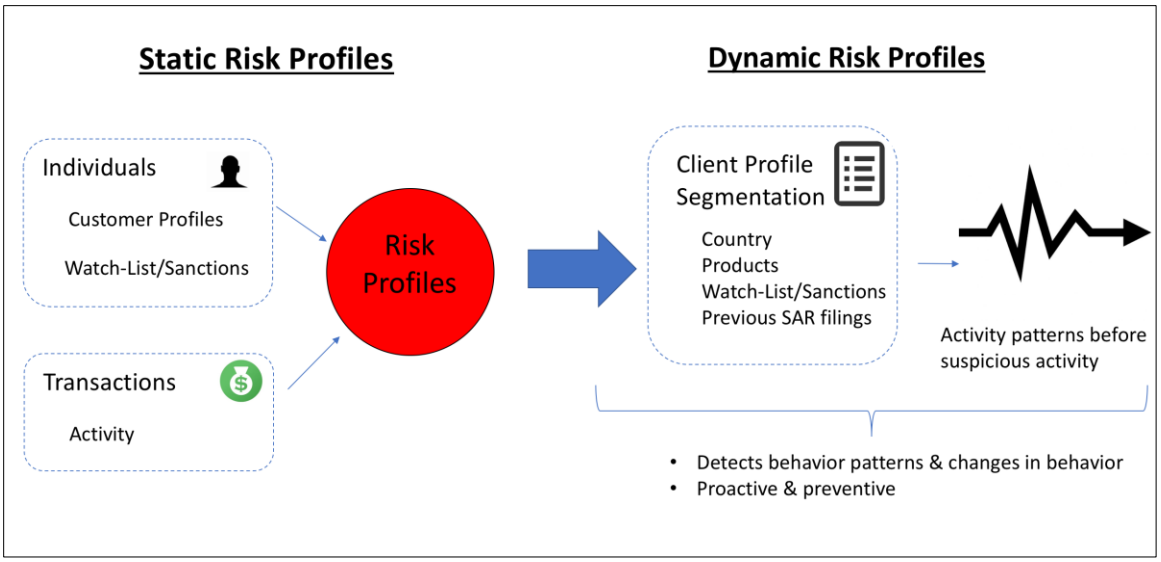
[l] Keys to an effective investigation process for this data include maintaining adequate files documenting reasons behind decisions to file SARs or not, performing enough due diligence on suspects or customers in addition to CDD/EDD documentation, and investigating the context of the transactions in question.

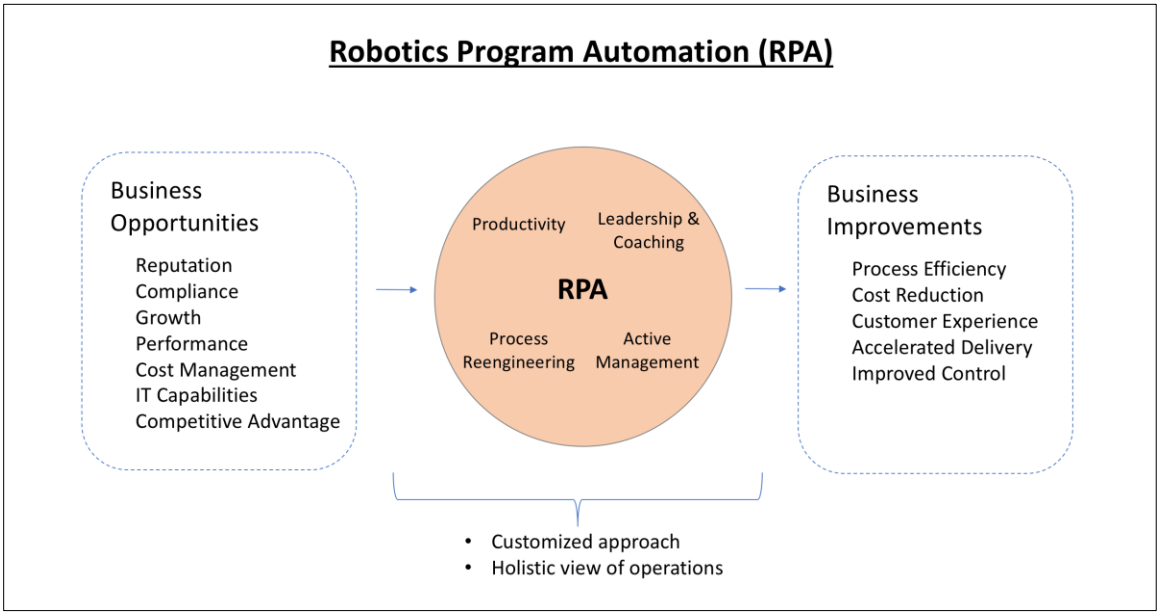
Implementing the right methodologies can greatly reduce work hours devoted to screening and investigation, allowing compliance staff to focus on higher level analysis and decision making. For instance, scenario logic validation construction requires specifying the right parameters, and utilizing adequate logic to match names with algorithms. Optimizing scenarios over time, particularly in threshold turning, will entail analyzing name masking algorithm outputs and threshold recommendations for escalating investigations.

2.2.2 Robotics for Dynamic Customer Profiles[16]

Robotics, designed based on inputs form several compliance officers, have also enabled dynamic customer profiles. Consistent updates keep KYC practices as secured, accurate, and complete as possible. Robotics program automation (RPA) can replicate human tasks for repetitive processes that involve navigating across applications, arranging inputs, and performing calculations. It can essentially make up a virtual workforce managed by business operations staff, and it can coexist with existing infrastructure at a financial institution. The benefits of these solutions include 24/7 automated solutions, estimated at 1/3 the cost of an average offshore employee workforce, with 100% accuracy in transaction execution. Overall, the payback period of installing RPA is estimated at less than a year, with a 70% cost reduction of data entry thereafter.

Robotics to Manage Customer Profiles





Source: "Integrating KYC Into the Digital Age and Enterprise-wide Transformation Strategy," ACAMS Webinar, March 7, 2017, https://www.acams.org/webinar-kyc-digital-age-enterprise-wide-transformation-strategy/.

Robotics can be designed for various purposes. As such, it can enhance other financial services and provide additional sources of data for suspicious activity, such as ensuring clients have the right products in their portfolios. Robotic checks are up to 22,000 times faster than manual checks and are based on suitability rules set by compliance staff. Long investigations of client investments can be greatly reduced, often by 1-2 hours each, freeing up compliance officers to perform high-level tasks for more value adding activities.[17]

Nevertheless, robotics alone cannot be expected to solve all AML issues, and the benefits are mostly in cost reductions and improved efficiencies. It is to this respect that robotics must be a component of a greater overall strategy for client lifecycle management, with the objective of risk mitigation and value creation across lines of business, financial products, and legal jurisdictions. Like robotics, artificial intelligence, one of the most complex technological solutions, uses neural networks and other intelligent technologies to consistently update customer profiles and allow close to real time analysis.

2.2.3 Network Analysis

Thousands of hidden relationships can be uncovered through tools that link data stored across dispersed sources of electronic information such as databases, PDF files, case management narratives, and web sites. These tools can enhance knowledge derived from customer profiles. For example, visualizations for entity resolution provide insight on clients' history with their networks and with a given financial institution. In addition, models of relationships through roles, processes, and interactions can be used for scenario analysis and preventive risk mitigation.

Linkages can be found and analyzed based on data that would otherwise be siloed in separate bank departments (retail banking, credit card, mortgage, business and investment accounts, etc.), adding to comprehensive customer profiles. For example, network analysis software can visually display connections of entire networks and group communities of connected individuals based on specific traits. Algorithms can be set to determine the strength of connections, as well as the likelihood and direction of network expansion. These solutions also allow for a better understanding of customer business relationships and external parties, according to KYC and Know Your Customer's Customer obligations.

3 Transaction Monitoring

3.1 Transaction Monitoring Challenges

3.1.1 Criteria and Systems

The purpose for monitoring suspicious activities is to red flag transactions originating from illegitimate sources. Transaction monitoring criteria should be calibrated to detect unusual activities and flows of funds. Yet suspicious activity monitoring and investigation programs can have information gaps, where details from transactions and risk assessments (customers, business lines, legal entities, etc.) are omitted.[m]

Individual system rules and thresholds can also be inadequately adapted to scrutinize high-risk business activities. Faulty detection logic can result from a lack of expertise necessary to design and fine-tune scenarios to cover red flags across an entire organization. This can lead to poor validation, alert, and case management systems. Often there is redundancy in system rules with overlapping conditions, where several different triggers can flag a single activity, which can lead to inefficiencies and duplicate investigations.

Moreover, because effective transaction monitoring relies on inputs from diverse business teams, deficient system functionalities may point to flaws in internal coordination across business lines and geographies. Cross-functional inputs are essential in defining the intended use of financial products, money laundering red flags, and typologies for transaction activities. A lack of collaboration among compliance, business, and technology teams hinders informed scenario creation by omitting essential expert evaluations on clients and the risks they pose to a financial institution.

A lack of information sharing in monitoring systems can lead to redundant cases and information asymmetries. This issue can escalate when the global reach of financial institutions can imply geographical distances among teams, coordination challenges, and discrepancies in regulatory requirements across legal jurisdictions. In this context it is difficult to manage and update quality rationale that will inform decisions to close, escalate, or document suspicions

[m] Common gaps in suspicious activity monitoring and investigation programs include incomplete monitoring of customers, transaction details, and relationships; flaws in developing and implementing suspicious activity monitoring policies; missing risk assessments to monitor suspicious transactions; lack of resources and training for investigation staff; and ineffective internal referral networks, use of monitoring technology, follow-ups on actions taken, and reporting to upper management.

from alerts. This is especially challenging when ensuring transaction monitoring systems are relevant on a local level. The consequences of these challenges can be deficient internal referral networks (ex: whistleblower hotlines), and failure to report key SAR details to senior management and board members.

3.1.2 Alert Systems

Transactions are becoming increasingly digital, a trend that is particularly manifested with merchants across industries conducting sales across various virtual touchpoints.[n] With e-commerce, mobile, and point-of-sale transactions relying on numerous digital payment methods, fewer in-person validations at the checkout counter can give way to new avenues of fraudulent activity.[18] Thus, multi-touchpoint interactions with customers require a multi-touchpoint approach to fraud detection. For instance, the rapid expansion of mobile payments raises particular risks, since transactions are highly automated and rely on saved user data.[19] In the alternative and peer-to-peer lending space, the regulatory "spaghetti soup" covering these transactions does not apply clearly or consistently to transaction activity. This ambiguity can also further criminal activity.[20]

Often, conventional rules-based AML systems, and even modern AML detection technologies, are based on logic that is too broad and not well aligned with actual patterns of fraudulent activity. This makes processes burdensome and can ultimately result in lost sales when legitimate fund transfers are declined or blocked for investigation. This calls for the more efficient filtering systems that can narrow down suspicious transactions where they are most likely to occur.

For this purpose, Suspicious Activity Reports (SARs) are meant to detect money laundering threats, providing red flags and evidence for AML risk assessments designed to address these threats. These risk assessments propose targeted actions, such as increased controls on alternative payment mechanisms (ex: funds transfers through mobile devices, pre-paid cards, cryptocurrencies, and third-party payment processors). However, inefficient alert systems can compromise the reliability of these risk assessments, hindering the precision of alert assignment and case management.[o] These inefficiencies lead to excessive SAR filings from internal referrals and other non-system sources, and by system redundancies that can activate multiple alerts from a single activity.

---

[n] Merchants are increasingly reaching out to target customers across varied touchpoints (Facebook, Instagram, Pinterest, Snapchat, etc.) aiming to facilitate sales transactions across devices (laptops, tablets, phones, etc.), through customers' payment systems of choice that directly rely on conventional card schemes (Visa, MasterCard, Amex, etc.) or other methods (PayPal, Apple Pay, Android Pay, wallets, etc.). In-person Different countries have different payment preferences, which further adds complexity to the potential risks of fund transfers.

[o] Indicators for evaluating the effectiveness of suspicious transaction monitoring programs include alert-to-case ratios, case-to-SAR filing ratios, non-system sourced cases-to-SAR filings, amount of alerts generated for certain products, transaction types, or high risk customers, varying degrees of clearing alerts by investigative personnel, whether disparate system rules generate alerts on the same activity, repeated SAR filings on the same subjects, backlogs and late SAR filings, and cases where auditors and regulators identify suspicious activities that went undetected on SARs.

Yet many financial institutions have not set up adequate systems to assign the most complex alerts and cases to seasoned AML professionals for review. This can compromise quality control, with a high variability among investigative personnel's rates of clearing alerts.[21] Poor alert management can entail unclear or missing SAR follow ups, contributing to repeated filings on the same subjects. Ultimately, backlogs and late SAR filings can reflect a range of complications that are magnified by poor customer termination decisions.

Excessive volumes of alerts generated from individual system rules/scenarios, and of SARs generated from these alerts, can also point to the issue of false positives. These alerts are eventually cleared rather than escalated, and they represent up to 95% of system outputs.[p] Low alert-to-case ratios and case-to-SAR filing ratios, as well as high percentages of repeated cleared filings, can point to excessive red flags, while false negatives point to undetected criminal activities due to missing alerts. Certain transaction types may not be covered in suspicious activity monitoring programs, resulting in a lack of necessary alerts. A shortage of alerts can be generated for high risk individuals and entities as a result of faulty risk assessment methodologies or ineffective integration of these risks into transaction monitoring software.

These inefficiencies in entity resolution encumber AML systems with manual practices of wading through volumes of false alerts before reaching the few that truly require scrutiny compromising the quality and completeness of investigation documentation, especially if manual processes could be replaced by automated systems that can process big data.

Tech Needs:

- Standardize transaction data collection and consolidation across business lines and geographies (ex: smaller offices in remote locations liaising with headquarters), linking to the 360-degree customer view.
- Incorporate AML industry and product expertise into system rules, with ongoing updates and effectiveness assessments to improve detection logic.
- Reduce false positives by improving filtering systems for suspicious activity. This requires optimizing parameters, data feeds, and staff training to either activate system rules or call for separate manual monitoring. Greater levels of efficiency will result from consolidating redundant monitoring rules, integrating non-system sourced cases (ex: media, law enforcement inquiries, etc.), enhancing current rules, and setting new rules based on patterns outside the scope of what current automated alerts can detect.
- Improve alert management decision making to promptly close, monitor, or escalate findings. This entails centralizing case management information, and potentially cloud computing capabilities to facilitate information sharing.[22]

[p] Legacy rules-based AML systems can generate 90% to 95% false positives, and the costs associated with following up on them has grown significantly over time.

3.2 Transaction Monitoring Solutions

3.2.1 Scenarios to Detect Suspicious Activity

Calibrated scenarios can effectively monitor activity based on specific traits such as transaction type, account, customer, household, and geography. Transactions are filtered by patterns, which could activate pre-determined alerts linked to decisions.[23] Certain queries can call for specific risk assessments (according to product or service, enterprise-wide, horizontal, line of business or legal entity, etc.). These risk-based scenarios can cover all customer activity, even spanning to third party transactions in order to monitor supply chains if necessary.[24]

To adequately detect irregular activity, scenarios must first define the conditions for "normal" activity that meets KYC standards, such that deviations will activate red flags given certain thresholds.[q] Crowdsourcing information can be a promising strategy to determine average patterns and eventually reduce the incidence of false positives.[r] Other inputs for standard activities can include expected customer behaviors and regulatory requirements. Deviations can be calibrated from red flags established by regulatory bodies and institutions, criteria from software vendors, lessons from affiliates and peers' experiences with similar customers, and internal data from past monitoring reports, investigations, SARs, and risk assessments.[s]

Scenario optimization relies on specifying the right parameters, designing replicable and adequate logic, and producing comparable outputs.[25] Along with subject matter expertise on data analytics, this is expected to minimize false positives and redundant scenarios.[t] Machine learning can enable systems to detect suspicious behavior and classify alerts as high, medium, or low risk, which can streamline case management and decision making.[26] Thus, improving alert scoring relies on software that can processes several forms of data. Rules-based software can identify and flag activities that violate predetermined rules, which are based on guidance from regulatory agencies or trade associations.[u] This technology detects known suspicious activity patterns (ex: structuring, fund flow-throughs, etc.). Effective red flag analysis also depends on adequate scenario coverage across products and services, geographies, and customer types.

---

[q] When establishing initial thresholds and tuning for new transaction monitoring systems, institutions need a customized approach, not a "plug-and-play." They should consider customer segmentation for cluster analysis, initial threshold setting, and threshold tuning over time. Much of this consists in determining normal conditions for details such as deposits/credits and withdrawals/debits per month, cash and wire transaction patterns, purpose of accounts, and destination of incoming/outgoing funds transferred. Custom profiles based on transaction activity can also be set using data on customer type (business or individual), geography, nature of business or occupation, account type (savings, checking, certificate of deposit, loan, etc.), balance, and transaction volume.

[r] Crowdsourcing can be an effective tool to determine answers to queries, using the "wisdom of the crowds," where averages of mass inputs can be more likely to be accurate than individual estimates.

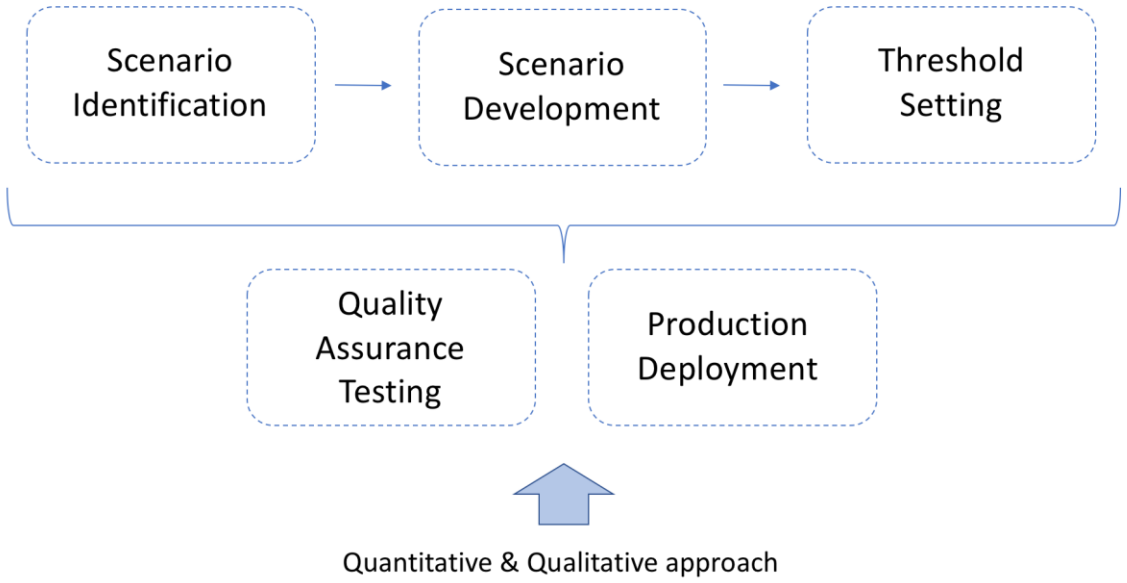
[s] In establishing scenarios, institutions should consider regulatory requirements, suspicious activity red flags set up by regulatory agencies, criteria of software vendors, affiliates and peers, historical reports/investigations/SARs, results of past risk assessments, and customer expected activity.

[t] Effective scenario tuning methodologies include statistical data analysis, initial testing in a tuning environment where volumes and effectiveness can be assessed, validation of effectiveness of samples depending on the number of false positives/negatives generated, above/below the line testing, and recalibrations for additional iterations.

[u] Guidance generally comes from institutions like FinCEN, the Federal Financial Institutions Examination Council (FFIEC), Joint Money Laundering Steering Group (JMLSG), Wolfsberg Group of Banks, and the Financial Action Task Force (FATF).

Beyond rules-based approaches, technological advances have incorporated customer segmentation in ways that allow targeted and behaviorally focused monitoring with the use of machine learning, robotics and detection algorithms. Artificial intelligence can also enable accurate comparisons between observed activity and established methods of money laundering activity, in order to identify suspicious activities, assess, and score them. AI depends on pre-established business rules and integrates them with sophisticated algorithms, leading to a more advanced and efficient solution than rules-based software.

Scenarios for AML



Source: Philip Tu, "Optimization of Technology to Meet Regulatory Expectations," ACAMS, https://www.acams.org/aml-white-paper-optimizing-technology/.

3.2.2 Predicting and Preventing Suspicious Activity

One benefit from digital transactions is the amount of data we can collect in order to fine tune detection systems and better target fraudulent activity.[27] For example, 3D Secure[v] technologies for customer authentication in transactions can be much more effective with pre-filtering systems that rely on dynamic automation. This added feature can more closely review customer history, update rules, and apply sophisticated matching logic to target only those activities most likely to involve crime.[28] Because the nuances that differentiate legitimate

[v] Define 3D Secure Is a protocol designed to add a layer of security to online credit and debit card transactions, through an additional authentication step in online payments. It relies on a 3-domain model: the acquirer domain involving the bank and merchant receiving a payment; the issuer domain involving the banks issuing the card used to make a payment; and the interoperability domain involving the infrastructure of card issuers.

transactions from fraudulent ones vary greatly by context (country, velocity, transaction size, etc.), machine learning tools can be key for a more accurate depiction of patterns of behavior.[29]

With a strategic use of data, predictive analysis can allow a fuller understanding of irregular activity in order to keep pace with criminal strategies. These capabilities can optimize detection and accuracy of alerts by integrating different technical methodologies.[w] Over time, systematic scenario tuning is essential for recalibrating parameters and iterating alert investigations using both quantitative and qualitative data. For example, testing parameter validation and effectiveness entails the analysis of the false positives and false negatives from a sample of alerts, which can give way to pattern recognition for future activity. Above/below the line testing also entails adjusting threshold values and re-executing cycles of alerts in order to compare with money laundering red flags and SAR typologies moving forward.

For rules-based software, conditions can be updated or customized with regulatory changes. Profiling software, on the other hand, can draw from past customer identification, customer due diligence (CDD), enhanced due diligence (EDD), and historical transaction data to create predictive profiles for future activity patterns. Transactions are flagged when they are deemed out of profile based on means, standard deviations, and thresholds, which can detect both known and unknown money laundering activities.

Moreover, artificial intelligence capabilities can consistently update and aggregate transaction data, so cumulative information can reveal the most up to date patterns of activity within and between accounts. These patterns can be extrapolated to predict future criminal trends and calibrate them into scenarios as deviations from future normal activity, and compared over time with actual outcomes to monitor effectiveness. Statistical data analysis identifies the critical traits of scenarios and determines threshold values to set. Threshold values can be tested, using resulting pilot alerts to assess volumes and effectiveness. When paired with visualization tools, decision making on the results of a set of transactions is greatly simplified.

4 Cryptocurrencies

4.1 Cryptocurrency Challenges

4.1.1 Use of Cryptocurrencies[x] for Criminal Activity

With evolving criminal methodologies, illicit users can become early adopters of new developments in financial products and services.[30] Cryptocurrencies, as a prime example, can be used to transfer funds derived from illegal activities and transnational crime.[y] Weaknesses

[w] Several different types of suspicious transaction monitoring software are available on the market. The most commonly used systems include rules-based, profiling, and artificial intelligence solutions, or combinations of all three.

[x] Cryptocurrencies are a form of digital currency, as are virtual currencies. These terms are not to be used interchangeably. Digital currencies are currencies that can be transferred and stored electronically. Virtual currencies are centralized and can be used primarily for online entertainment in virtual worlds, which are not based on physical reality. Cryptocurrencies are meant to be able to replace cash and are generally decentralized.

[y] Heightened money laundering and terrorist financing risks of these currencies and the systems they run on include their use for financial crimes (fraud, identity theft, account takeover, money laundering), financing illicit activities (purchase of illicit

in system infrastructure, combined with a lack of expertise on user roles and third-party providers, allow for obscure money trails and even fraudulent mining. While the legal community disagrees on whether cryptocurrencies[z] are technically a form of money,[31] these emerging value transfer mechanisms are subject to "laundering" when funds are moved in ways that obscure their original source (ex: funds moved from an address associated with crime to another address, or cashed out as fiat currency).

Cryptocurrency laundering can be simpler than conventional money laundering because "cleansing" wealth from its illegal source requires less steps and all takes place within a single blockchain ecosystem before cashing out. There is no separate legitimate financial system to integrate dirty funds into.[aa] Moreover, parties involved in these transactions tend to be anonymous, making this a preferred system of exchange for criminal activity. Cryptocurrencies and the systems on which they operate could thus pose increasing money laundering risks as their use becomes more prevalent.[32] Though it is impossible to measure the exact value within these exchanges that derives from criminal activity, we can still observe common patterns of use and discover typologies for laundering.

Using Bitcoin as a case in point, [bb] the first cryptocurrency laundering study of its kind uses transaction data from 2013-2016 to identify movements of illicit funds.[33] While less than 1% of transactions directly entering funds into conversion services[cc] involved illicit entities (intermediaries aren't covered), the number of these entities increased five-fold. Out of 102 illicit entities detected, only 9 processed over 95% of laundered Bitcoins. They were all darknet marketplaces, by far the greatest source of illegal wealth (97.36%). The competitive landscape of illicit entities may represent a monopoly transitioning into an oligopoly, with increasing levels of fragmentation[dd] following the major shutdowns of Silk Road in 2013[34] and AlphaBay in 2017.

Furthermore, the observations from the study show that exchanges receive the highest amount of overall bitcoin transactions entering conversion services (75%). Accordingly, they also process the most robust volume of illicit wealth, representing 45% of Bitcoin laundering, even though this represents only 0.61% of total Bitcoin exchange transactions. Mixers and gambling services, on the other hand, have a much higher propensity to receive dirty Bitcoins. Mixers

---

goods or services, and transferring donations to transnational criminal organizations), fraudulent mining methods, movement of illicit funds across borders, lack of transparency due to anonymity (use of avatars and fake identities), difficulty in sanctions screening, lack of historical legal oversight, lack of compliance experience among staff, system weaknesses and limited understanding on the technical infrastructure, lack of centralized administration, and third-party service providers (exchangers, wallet services, etc.) that can further obscure money trails.

[z] FinCEN defines "virtual currency" as "a medium of exchange that operates like currency in some environments, but does not have all the attributes of real or fiat currency."

[aa] Conventional money laundering ends in a final step of integrating dirty funds into the legal financial system by means of various transactions intended to confuse and make the "dirty money" seem "clean."

[bb] In being the first virtual currency released in 2009, Bitcoin has the longest history of transactions.

[cc] Conversion services refer to platforms and intermediaries that transmit funds on behalf of users, either by cashing out bitcoins to currencies with legal tenders, converting to other cryptocurrencies, or transmitting them to other Bitcoin address, potentially in ways such that the flow of funds can't be traced directly on the blockchain. Examples of conversion services include virtual currency exchanges, mixers, online gambling sites that accept cryptocurrency, and Bitcoin ATMs.

[dd] In the last few years, with the Locky RansomWare attack and the OneCoin scheme of 2016, ransom and Ponzi schemes have also seen an increase as a source of illicit funds. Yet they still represent a small percentage of overall criminal funds.

process funds from illicit sources at a rate of over 20% since 2013, followed by a sharp drop in 2016, which can reflect an overall fall in the proportion of illicit funds as virtual currencies become more popular in the mainstream market. Gambling services process fewer but larger transactions. Finally, conversion services based in Europe and in undisclosed jurisdictions processed a combined amount of bitcoin laundering activity ranging from 86-93%.

4.1.2 Compliance

Cryptocurrency exchanges are in practice considered money service businesses (MSBs), and as such are expected to adhere to AML compliance standards. They must establish AML programs that meet the stipulations of the USA Patriot Act, as well as FinCEN rulings for money transmitters dealing with these currencies.[ee] Yet structural differences from conventional money systems can present difficulties in identifying the applicability of existing AML regulations. For instance, certain parties engaging with these currencies are not considered money transmitters and may not be subject to compliance requirements that would be adequate for their role. These parties include miners, investors, software developers, and businesses that rent computer systems for mining. Financial institutions engaging with cryptocurrencies, and the web of relationships they involve, can be left to identify and manage these risks on their own. This can be a very challenging task.

Moreover, de-centralized cryptocurrency systems have no single administrator or repository, and users are only subject to AML/CFT requirements of money transmitters when transferring value between entities or across locations.[35] The personal use of these currencies, which includes the purchase of goods and services, is not subject to these rules. This can leave a significant portion of transactions largely unregulated, and thus conducive to illicit activity. The lack of a centralized supervision can also facilitate concealing user and transaction information essential for investigations and law enforcement. This can lead to inadequate sanctions screenings and a lack of oversight, where the level of anonymity in the system can endorse activity that would otherwise call for currency transaction reports (CTRs) and suspicious activity reports (SARs). Fund movements can be impossible to trace, particularly when they involve many players and complex transactions, as is often the case in the blockchain.

To add to these compliance challenges, there is still a limited understanding of digital currencies' usage for money laundering activity, which contributes to the historical lack of oversight as of today. Institutions disagree on whether and to what extent cryptocurrencies present risks, which can be a reason for the low overall levels of cryptocurrency-specific regulation. Consequently, AML compliance experience among operators and employees of cryptocurrency systems can be limited, especially when they deal with multiple jurisdictions that present varying regulatory requirements.

[ee] According to Section 352 of the USA Patriot Act, virtual currency exchangers and administrators are required to establish AML programs because they fall under the category of money transmitters, which provide services defined as "the acceptance of currency, funds or other value that substitutes currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means."

4.1.3 Legacy Technology

Legacy technology, considered a barrier to fighting financial crime in the immediate future, creates concern for organizations lacking the technical capabilities to detect and stop illegal activity.[ff] This is especially the case with new developments that financial institutions must keep up with as they engage with cryptocurrency users and exchanges. Thus, inefficiencies observed in transaction monitoring have made reforming suspicious activity reporting a main AML priority identified by the US Treasury Department and other regulatory bodies across jurisdictions.[gg] Outdated systems, often inherited through past mergers and acquisitions, need to be updated across entire institutions. Otherwise, ongoing patchwork upgrades can pose future operational and risk management costs, or even loss of business. These updates don't achieve the necessary scale to stay ahead of criminal methods, leaving system vulnerabilities to crime that are preventable with the right implementation of existing technologies.[36]

One particular area of AML concern is cybercrime,[37] given the pace of developments among criminals who can rent botnets capable of bringing down entire networks. Banks recognize cybercrime as the top area of investment in financial crime prevention moving forward, by far exceeding expected investments in fraud and overall AML.[hh] As of yet, they don't feel fully equipped to protect themselves. There is an increasing need for AML compliance officers and information security teams to understand cybersecurity and develop effective plans to address, mitigate, and report potentially adverse cyber-events in the context of new technologies.[38]

Tech Needs:

- Gather and aggregate information on clients, transactions, and suspicious activity patterns, in order to define what criminal activity entails in the blockchain.
- Balance personal privacy safeguards while keeping information available for law enforcement.
- Integrate technological innovation with regulatory developments, so regulation can ideally embrace regtech adoption for AML for more consistent compliance measures. This requires deepening expertise on the functionality and risks of these currencies, as patterns of use and typologies of crime are better established.

4.2 Cryptocurrency Solutions

4.2.1 Tools to Detect Suspicious Activity

Cryptocurrencies are easily downloadable, open-source software generally on a decentralized network, which offers ease of use and potential widespread adoption. As an alternative

[ff] In a survey of UK institutions conducted by LexisNexis in 2017, 23% of respondents admitted they were very concerned about legacy technologies unable to detect financial crime, and 69% admitted to being somewhat concerned. The UK market is in many ways analogous to the US market, so it is safe to assume that this trend would be similar in the US.

[gg] The US Treasury Department has updated its national money laundering risk assessment in 2015, setting a precedent for other regulators around the world including the UK.

[hh] Cybercrime prevention is expected to be a top area of investment in the near future. Among UK Institutions, 39% of survey respondents acknowledged this, and for retail/wholesale banks, 67% did so. A greater awareness among financial institutions regarding their shortcomings in keeping pace with cybercrime is correlated with higher perceived needs for investment (70% for banks vs. 50% for all UK respondents).

payment method, cryptocurrencies inevitably present risks of illicit finance when introduced to the public. The technology to monitor transparent ledgers is still under development, as is the level of overall understanding on the indicators of suspicious activity. One potential benefit of this highly automated ecosystem is the ability to gather massive amounts of data. Data analytics allow the financial community to continues defining typologies of illicit patterns to investigate and red flag. Cases, scenarios, and thresholds can be set for automated and robotics solutions to filter activity. For example, Citigroup, Bank of America, and other large banks have already begun testing blockchain solutions to shut out cybercriminals.[ii]

Here is where subject matter expertise (SME) can be invaluable in assessing patterns, the blockchain technologies they operate on, and the technologies to monitor them, particularly where decision making can be most challenging. While the right technologies may exist and be available, financial institutions may need specialized guidance in order to best implement them. Investors backing new technologies can also help determine the true value of new developments. In this respect, a number of blockchain solutions to cybercrime and overall cryptocurrency crime have been implemented successfully, leveraging decentralization to provide platforms that foster trust such as smart contracts and secure transaction systems.

Technological tools such as these can assess particular risks and vulnerabilities depending on the type of cryptocurrency system evaluated (closed, unidirectional, bidirectional, centralized, or decentralized), the individuals and entities using it, and the transaction volume they mobilize. For example, banks can assess the risk of customers administering and exchanging cryptocurrencies by screening for machines that perform automated illicit transactions. This requires tools that ensure human triggers to activate system functionalities, as well as notifications of ownership changes and shipments linked to unusual activity. Much like in conventional AML systems, geographical considerations may also point to heightened risk based on location of business operations, customers, and transaction origin and destination.

Financial institutions can leverage these internal compliance systems to cooperate with law enforcement, aggregating data from various sources to better identify industry trends and enhance overall detection capabilities. [39] As financial institutions invest in systems to mitigate cyber threats, regulation also comes to target cybersecurity.[jj] Institutions must comply with rules for identity “red flags” in customer screenings and prepare to undergo examinations on their preparedness for cyber threats. In the realm of cryptocurrencies, implementing written identity theft prevention programs can be key to detect, prevent, and mitigate breaches. Thus, through an adequate use of data and risk management technologies, the cryptocurrency space can be better monitored and regulated.

[ii] These blockchain solutions also have the potential to reduce costs.

[jj] In October of 2016, FinCEN released an advisory publication on cybercrime, discussing concerns of cyber-events and cyber-enabled crimes for financial institutions, and providing guidance on filing suspicious activity reports (SARs). The SEC and the CFTC have also released guidance on cybersecurity and customer data protection in an attempt to safeguard digital identities.

4.2.2 Screening Cryptocurrency Users

Technology can enhance due diligence measures for individuals and entities acting as currency exchangers and system administrators.[40] For example, verification services can cross-reference records to authenticate corporate documentation, licenses, permits, contracts, and references. These tools can also review users' relationships with other financial services providers transferring funds on behalf of cryptocurrency systems and users. Automation can further screen public databases to identify cryptocurrency addresses, principal owners, and marketing campaigns linked to risky activities.[kk] Specifically robotics can detect patterns and perform predictive analysis to allow expected versus actual comparisons, using indicators such as transaction volumes. Other calibrations can simulate tests with controls and constraints, such as comparisons across users within a single geographic location or demographic category.

With the right analytics in place, alerts can be calibrated to flag unlicensed or unregulated customers, or information gaps where more robust licensing and regulation is needed. These customers may be unaffiliated with conventional financial institutions, and instead be linked to high risk nonbank financial institutions such as casas de cambio. They may also operate in high risk jurisdictions or areas with lax AML regulations. Cryptocurrency systems with lax or inexistent customer identification and monitoring procedures enable greater potential anonymous illicit transactions, which automation can detect.

Yet because screening requires sorting through personal information, privacy measures are imperative to safeguard sensitive data and prevent breaches. Robust identity safeguards can be key to expanding the legal use of cryptocurrencies, while providing the data necessary for AML initiatives and compliance to trace transactions when needed. For example, Zcash is an attempt to balance the need for privacy and the ability to enforce regulation. The zero-knowledge proof system of its blockchain is a cryptographic innovation over the basic bitcoin system that allows users to shield sensitive information from the public ledger; it still gets recorded in the blockchain, so it's accessible for law enforcement in cases of investigation.[41] While disclosure of details on users and transactions can be kept private, transactions can still be audited. As other innovations are yet to be determined, cryptocurrencies may survive and even flourish to the extent that safeguards are put in place to address criminal use.

5 Conclusion

Evolving criminal methodologies represent by far the largest financial crime risk identified by organizations, today and in the future. The most pressing challenges for managing AML programs moving forward can be traced to this risk in relation to the resulting/daunting regulation that financial institutions are obliged to comply with, the demands to innovate existing systems and implement new technologies, and the need for adequate human resources to manage the use of innovation and make informed decisions. Financial institutions are rapidly implementing AML solutions in strategic ways that can both mitigate crime and facilitate compliance.

[kk] Examples of these activities include illegal Internet gambling, unregulated pharmaceutical companies, escort services, get-rich-quick investment schemes.

Yet this presents significant costs to meet the increasing volume and complexity of regulatory requirements, while making necessary investments in human resources and technology. When something does go wrong, the reputational costs of illegal activities going undetected may even be more severe than the monetary charges.

Furthermore, US regulatory agencies have been aggressively stepping up enforcement actions, imposing severe penalties for compliance failures. OFAC-related settlements are particularly daunting, with the largest up to date being of $8.9 billion imposed by US courts on BNP Paribas in 2015 for failing to comply with sanctions measures.[42] The US Treasury Department has authority to pose major restrictions on anything it deems to be a "primary money-laundering concern." Ultimately, the onus for failing to address these deficiencies in AML programs lies on the individuals behind them.[43] Beyond the civil and monetary penalties levied on bank directors and senior management, compliance professionals are deemed personally liable for the actions they oversee.

In the case of breaches, compliance officers are at risk of facing huge repercussions, and CCOs especially are put under scrutiny because they could be made fully responsible for oversight. This creates an environment that can be more conducive to avoiding penalties than fostering innovation/cooperation for proactive AML solutions. There is a widespread perception in the financial community that there is a lack of skilled senior leaders to confront AML challenges, while front-office personnel fail to prioritize middle or back-office compliance needs due to a lack of organizational buy-in.

As financial institutions may not have all the resources to manage these changes in-house, it can be more cost-effective and practical to rely on outside subject matter expertise to provide guidance on effective compliance and implementation of tech solutions available to meet an institution's specific AML needs. Compliance assessments are best carried out by Subject Matter Experts who have the skills, grace and experience to navigate these complexities with proven experience working with various FIs, verticals, industries along valuable exposure to next-generation technology in ways that will fosters in-house compliance knowledge.

UGR Consulting is a leading and visionary boutique consulting firm which provides SME advisory with innovative solutions and next generation technology to meet the challenges of the financial services industry. We help smaller banks have a more customized approach along expertise to evaluate at best their risk metrics while remaining cost efficient. On the other hand, larger institutions may want to equip their in-house teams with SMEs and improve scale efficiencies while having expertise for needed only projects without going through the hassle of hiring full time employees without compromising quality and integrity.

SMEs are the answer to today's compliance needs because they not only have gathered experience and expertise as former professionals (former CCO, Compliance & AML experts etc..) but also have the holistic mindset of evaluating risk factors all together and bring value added solutions to specific cases and scenarios.

References

1 "Basel Index AML Report 2017," Basel Institute on Governance, August 16, 2017, https://index.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2017.pdf.

2 "Guide to US Anti-Money Laundering Requirements," Protiviti, https://www.protiviti.com/sites/default/files/united_states/insights/guide-to-us-aml-requirements-6thedition-protiviti_0.pdf.

3 Tim Lloyd, "ACAMS' Top 5 Predictions for AML in 2018," Thomson Reuters, https://legalsolutions.thomsonreuters.com/law-products/solutions/clear-investigation-software/anti-money-laundering/ACAMS-top-5-predictions-for-AML-in-2018.

4 "History of Anti-Money Laundering Laws," FInCEN, https://www.fincen.gov/history-anti-money-laundering-laws.

5 "Country guides: Securities and Banking," WilmerHale, May 12, 2015.

6 "Country guides: Money Laundering," Protiviti, December 10, 2014.

7 "FInCEN Finalizes Customer Due Diligence Rule for Legal Entity Customers," Morrison & Foerster, May 16, 2016, https://media2.mofo.com/documents/160516fincen.pdf.

8 "Five steps for anti-money- laundering compliance in 2017," Alix Partners, February 2017, https://www.alixpartners.com/insights-impact/insights/five-steps-for-anti-money-laundering-compliance-in-2017/#sm.0001tgb42i15ndcx5zzcqgmpq1isy.

9 Stacey English and Susannah Hammond, "Fintech, Regtech, and the role of Compliance 2017" Thomson Reuters, https://risk.thomsonreuters.com/en/resources/special-report/fintech-regtech-and-the-role-of-compliance-2017.html.

10 "The Challenges of Managing a Global AML Program: Distinctions Across the United States, the United Kingdom, and Hong Kong,," Protiviti, https://www.protiviti.com/sites/default/files/united_states/challenges-managing-global-aml-program-protivit.pdf.

11 Trisha Dutta, "Build an Integrated 360-Degree View of the Customer," IBM, August 22, 2014, http://www.ibmbigdatahub.com/blog/build-integrated-360-degree-view-customer.

12 "Global Business Trends: Protecting Growth Ambitions Against Rising Fraud Threats", Experian, http://www.experian.com/decision-analytics/global/reports/fraud-report.html.

13 "Guide to US AML Requirements 6th Edition," Protiviti, https://www.protiviti.com/sites/default/files/united_states/insights/guide-to-us-aml-requirements-6thedition-protiviti_0.pdf.

14 "Ten things compliance officers need to do in 2018," Thomson Reuters, https://risk.thomsonreuters.com/en/resources/expert-talk/10-things-compliance-officers-need-do-in-2018.html.

15 Margo Vakharia, “Leveraging Big Data Techniques to Enhance Anti-Money Laundering Practices,” ACAMS, http://files.acams.org/pdfs/2017/Leveraging_Big_Data_Techniques_to_Enhance_M.Vakharia.pdf.

16 “Integrating KYC Into the Digital Age and Enterprise-wide Transformation Strategy,” ACAMS Webinar, March 7, 2017, https://www.acams.org/webinar-kyc-digital-age-enterprise-wide-transformation-strategy/.

17 Alex Davidson, “Credit Suisse offers glimpse of future role of compliance officer in banking,” Thomson Reuters, January 29, 2018.

18 “Optimizing Payments for Omnichannel Commerce: 5 Best Practices,”Adyen and Edgar, Dunn & Company, https://www.adyen.com/knowledge-hub/white-papers/optimizing-omnichannel-payments

19 Pierre-Laurent Chatain, Andrew Zerzan, Wameek Noor, Najah Dannaoui, and Louis de Koker, “Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions,” World Bank, February 24, 2011, https://openknowledge.worldbank.org/bitstream/handle/10986/2269/600600PUB0ID181Mobile09780821386699.pdf.

20 Karen Gordon Mills and Brayden McCarthy, “The State of Small Business Lending: Innovation and Technology and the Implications for Regulation,” Harvard Business School, October 27, 2016, http://www.hbs.edu/faculty/Publication%20Files/17-042_30393d52-3c61-41cb-a78a-ebbe3e040e55.pdf.

21 “The Challenges of Fighting Money Laundering,” June 30, 2016, Pitney Bowes, https://www.complianceweek.com/thought-leadership/ebook/e-book-the-challenges-of-fighting-money-laundering#.Wre9NWWka-Q.

22 Kevin Harris, “Implementing an Effective Anti-Money Laundering System,” ACAMS, http://files.acams.org/pdfs/2016/Implementing_an_Effective_Anti-Money_Laundering_System_K_Harris.pdf.

23 “2018: The Year Ahead in AML Compliance, Insights on the AML and Sanctions Landscape for US Financial Institutions,” Protiviti Webinar, January 11, 2018, https://www.protiviti.com/sites/default/files/united_states/insights/2018_the_year_ahead_in_aml_presentation_protiviti.pdf.

24 Philip Tu, “Optimization of Technology to Meet Regulatory Expectations,” ACAMS, https://www.acams.org/aml-white-paper-optimizing-technology/.

25 “Cybersecurity & Vendor/Third Party Risk. From Predictive Insight to Action,” Aravo Webinar, February 27, 2018, https://explore.securityscorecard.com/Aravo_Cybersecurity-and-Vendor.html.

26 “Are Artificial Intelligence And Machine Learning The Next Frontiers For Fighting Money Laundering?,” Forbes, January 16, 2018, https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/steveculp/2

018/01/16/are-artificial-intelligence-and-machine-learning-the-next-frontiers-for-fighting-money-laundering/&refURL=&referrer=.

27 Attila Dogan, "Fighting Fraud With Unified Data," Adyen, https://www.adyen.com/knowledge-hub/white-papers/fighting-fraud-with-unified-data.

28 "How to Win With Dynamic 3D Secure," Adyen, May 1, 2017, https://www.adyen.com/blog/how-to-win-with-dynamic-3d-secure.

29 "Stripe Snapshot: Online Fraud Trends and Behavior," December 12, 2017, https://stripe.com/files/blog/stripe-snapshot-fraud.pdf.

30 Andrew Wagner, "Digital vs. Virtual Currencies," Bitcoin Magazine Issue 22, August 22, 2014, https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507/.

31 Andrew Tar, "Digital Currencies vs. Cryptocurrencies Explained,," Cointelegraph, December 13, 2017, https://cointelegraph.com/explained/digital-currencies-vs-cryptocurrencies-explained.

32 Steve Hudak, "Treasury's First Action Against a Foreign-Located Money Services Business," July 27, 2017, https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.

33 Yaya J. Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services," Foundation for Defense of Democracies' Center on Sanctions & Illicit Finance (CSIF), Elliptic, January 12, 2018, http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.

34 Jose Paglieri, "FBI Shuts Down Online Drug Market Silk Road," CNN Money, October 2, 2013, http://money.cnn.com/2013/10/02/technology/silk-road-shut-down, accessed May 1, 2014.

35 "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies FIN-2013-G001," FinCEN, March 18, 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

36 "Future Financial Crime Risks 2017," LexisNexis, https://risk.lexisnexis.co.uk/insights-resources/white-paper/future-financial-crime-risks-2017-wp-uk.

37 Susannah Hammond, "Five key risks for firms in 2018," Jan 17, 2018, https://blogs.thomsonreuters.com/answerson/five-key-risks-firms-2018/.

38 Glen Kopp, "New York DFS Finalized Cybersecurity Regulations Take Effect," Corporate Compliance Insights, March 27, 2017, http://www.corporatecomplianceinsights.com/new-york-dfs-finalized-cybersecurity-regulations-take -effect.

39 Joe Soniat, "Cybersecurity and BSA/AML," ACAMS Today, June 9, 2017, https://www.acamstoday.org/cybersecurity-and-bsaaml/.

40 Sherri Scott, "Cryptocurrency Compliance: An AML Perspective," ACAMS, http://files.acams.org/pdfs/2017/Cryptocurrency_Compliance_An_AML_Perspective_S.Scott.pdf.

41 “New Blockchain Platforms Emerge to Fight Cybercrime,” Forbes, November 13, 2017, https://www.forbes.com/sites/rogeraitken/2017/11/13/new-blockchain-platforms-emerge-to-fight-cybercrime-secure-the-future/#59bffac168ad.

42 Nate Raymond, “BNP Paribas sentenced in $8.9 billion accord over sanctions violations,” Reuters, May 1, 2015, https://www.reuters.com/article/us-bnp-paribas-settlement-sentencing/bnp-paribas-sentenced-in-8-9-billion-accord-over-sanctions-violations-idUSKBN0NM41K20150501.

43 Stacey English and Susannah Hammond, “Cost of Compliance 2017,” Thomson Reuters, https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/report/cost-of-compliance-2017.pdf.