ManagementSolutions
Making things happen

Financial Crime: challenges and trends in the digital era

R&D

www.managementsolutions.com

Design and Layout
Marketing and Communication Department
Management Solutions

Photographs
Photographic archive of Management Solutions
iStock

Contents

Introduction

"Crimes carry punishment on their backs"
Miguel de Cervantes[1]

Financial Crime is a general concept that comprises a set of illicit activities. Although there are differences across jurisdictions, in general terms Financial Crime includes activities such as money laundering (i.e. transforming into legal the money that comes from different illegal activities), terrorist financing, breach of economic sanctions, bribery and corruption, fraud, and market abuse[2].

Financial Crime and money laundering (ML) is a major threat that the financial sector faces in their risk identification, management, and control frameworks. For example, focusing on ML, the amount of money laundered globally in a year is estimated to reach between 2% and 5% of global GDP, or between $800 billion and $2 trillion in current US dollars[3]. However, less than 1% of it is ever seized or frozen by law enforcement agencies[4].

In the last years, financial institutions from many different geographies invested billions of dollars in improving their systems, people and processes to be able to tackle the increasing threat that Financial Crime poses to their stability and to their reputation. According to some industry reports, the yearly investment in Financial Crime compliance across financial institutions worldwide is estimated to be more than $200 billion[5].

Several factors make the tackling of Financial Crime increasingly challenging, including:

- An ever more global economy and corresponding interconnected financial sector, that makes it challenging to perform a full traceability of money.
- Local approach to supervision. Historically, the approach to Financial Crime, and in particular the activities of AML, has been driven by local legislators and supervisors, country-specific law enforcement authorities, and financial intelligence agencies. Despite the existence of inter-governmental bodies, such as the Financial Action Task Force[6], there has been no operational platforms, nor regulatory and supervisory mechanisms for effective collaboration and information sharing.
- The progressive sophistication of the money laundering strategies, involving other types of crimes such as fraud or cybercrime (e.g. identity theft)[7].
- The evolution of the payments industry towards easier, quicker and more flexible digital payments mechanisms.
- The irruption of cryptocurrencies and their ability to avoid traceability of the sources of funds[8].
- The technological advances deployed as a result of the pandemic, which have forced financial institutions to reduce face-to-face interactions and substitute them by digital processes (including remote onboarding of new clients), more susceptible to digital crime that can eventually lead to Financial Crime.

Notwithstanding, financial institutions have strong tailwinds and can reach more powerful tools to effectively fight against Financial Crime, by identifying, monitoring, measuring, and controlling these types of illicit activities, including:

- Stronger computational capacity to execute risk identification alerts and strategies in real time involving a much richer set of data points to identify sophisticated strategies.

[1] Miguel de Cervantes Saavedra (1547-1616). Spanish writer. Author of the work "El ingenioso hidalgo Don Quijote de la Mancha".
[2] Financial Conduct Authority (2021).
[3] United Nations Office on Drugs and Crime (2011).
[4] World Economic Forum.
[5] Lexis Nexis Risk Solutions (2021).
[6] A cross-government action group gathering more than 200 countries, and that acts as the global money laundering and terrorist financing standard-setter),
[7] A paradigmatic example of cybercriminals Carbanak and Cobalt can be discussed: gangs of criminals are able to (i) insert a malware in the work accounts of banks employees (through standard phishing techniques – cyberattack); (ii) use credentials to increase balances of certain accounts (fraud); (iii) allow the money to be transferred cross border and/or extracted through ATMs; and (iv) reinsert it in the system using classical money laundering techniques. See Europol media release https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
[8] Paesano, F. (2021).

- More advanced mathematical modelling, including ML algorithms that can run quicker and are able to refine the strategies and improve effectiveness in the detection.

- Increased awareness from the C-suite and Board of the implications of this type of crimes, which grants multi-year commitment and investment. At the same time, increased visibility of the total cost of Financial Crime (including both direct losses, and those from remediation and fines[9]), as well as awareness of the ever more 'connected' Financial Crime risks.

- Increased collaboration intra-company, with the removal of silos and the collaboration across departments (technology, compliance, legal, money laundering prevention, sanctions, etc.) to ensure that there is full information sharing and transparency across teams in charge of Financial Crime.

- From the early work of the International Financial Task Force, and with the work of other international organizations such as the United Nations Office on Drugs and Crime, there is much more awareness around the importance of international cooperation.

Anti-Money Laundering and Counter Terrorist Financing (AML/CTF)

One of the activities to prevent Financial Crime that have attracted particularly large investments in the last years is AML/CTF, after a series of very notorious cases affecting large Global Systemically Important Banks, and the corresponding stronger regulatory scrutiny[10,11]. However, despite the significant progress made in the reinforcement of those capabilities, the prevention of these illicit activities remains today one of the main areas of concern for financial institutions.

Given the cross-border nature of the money laundering and terrorist financing, one of the most instrumental tailwinds is stronger international cooperation across countries and regions to perform synchronized action.

In that line, regulators and supervisors are paying a key role in encouraging and enabling such global collaboration and supporting overall the prevention of these crimes. Some of the examples of regulatory action include:

a. Strengthening the supervisory mechanisms to cut across jurisdictions. For example, EU's 5th Anti-Money Laundering Directive[12] requires that the EC performs a biannual assessment of the risks of ML/TF that could impact the internal market in the region[13]. The outcomes of such assessments inform regional and local policymakers.

b. Encouraging for a higher cooperation between local legislators and supervisors, country-specific law enforcement authorities and financial intelligence

[9] Lexis Nexis Risk Solutions (2021).
[10] Sanction Scanner (2021).
[11] European Commission (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0373
[12] European Parliament and the Council (2015).
[13] See, for example, the EU Commission's Supranational Risk Assessment Report and the Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.COM (2019) 370. See also the UK's National risk assessment of money laundering and terrorist financing 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf

agencies[14]. The 5th EU AML Directive[15] requires an assessment, by the EC, of the framework for cooperation between Financial Intelligence Units in the EU European Union, and with third parties. The Directive includes the possibility of establishing a coordination and support mechanism. In that line, recently the EU announced the creation of a new EU authority[16] to enhance AML/CTF supervision and cooperation across local Financial Intelligence Units (FIUs). The so-called AMLA[17] will act as a central authority and will coordinate national authorities to ensure, amongst other things, that each country's private sector adequately applies EU rules. As a continuation of that effort, the EBA recently published its 'Guidelines on cooperation and information exchange between prudential supervisors, AML/CTF supervisors and financial intelligence units under Directive 2013/36/EU'[18].

c. Pursuing the collaboration between prudential and non-prudential supervision[19].

d. For emerging risks or areas of weakness identified as part of its supervisory process, regulators around the world are being very active in terms of issuing new regulation. One of the areas of more rapid evolution is that of cryptocurrencies[20].

e. Encouraging the investment in data, advanced modelling and AI, including advanced outlier analysis, and graph analytics for the modelling of networks and multiple order relationships[21].

In this context, the purpose of this white paper is twofold:

- Define the area of Financial Crime and analyze the regulatory context.
- Develop a special focus on the challenges and trends in AML/CTF, including the response from financial institutions to improve the risk management and control frameworks, and establish some relationships between AML/CTF and other risks that comprise the concept of Financial Crime.

The document is structured as follows: after an executive summary, section 2 contains an overarching view of the concept and regulatory landscape about Financial Crime. Section 3 covers the main challenges and trends in AML/CTF, including the framework and governance, the organizational design, the data needs, the business processes, and technological infrastructure. Finally, section 4 contains a specific focus on advanced mathematical modelling capabilities and trends used for the purpose of improving efficiency and effectiveness in AML/CTF detection.

[14]European Banking Authority (2021).
[15]European Parliament and the Council (2015).
[16]European Parliament (2021).
[17]Not to be mistaken for The US Anti Money Laundering Act (2020)
[18]European Banking Authority (2021).
[19]Mersch, Y. (2019). Anti-money laundering and combating the financing of terrorism – recent initiatives and the role of the ECB.
[20]European Banking Authority. (2021).
[21]Financial Conduct Authority (2022). Regulatory Sandbox.

Executive summary

"Capital is not an evil in itself, the evil lies in its misuse"
Mahatma Gandhi[22]

1. ***Definition***. Financial Crime is a broad term that refers to a set of non-prudential risks that organizations in the financial sector face as part of their business origination activities. Amongst others, Financial Crime includes laundering money coming from different illegal activities (including drug, arms or human trafficking, slavery, etc.), the financing of terrorism, breach of economic sanctions, bribery and corruption, Fraud, and Market Abuse. Lately, cyber-risk and digital crime has also been included in this category.

2. ***Focus.*** Whilst all of those sub-risk types have received a lot of attention and investment in the last years, this analysis will be focused on three sub-risk types that tend to be treated under similar frameworks by organizations: money laundering, terrorist financing and economic sanctions. Following industry and regulatory standard convention, this document refers to it generically as AML/CTF (Anti-Money Laundering and Counter Terrorist Financing). The rationale for focusing on AML/CTF, in addition to allowing for more depth of analysis, also responds to the increasing regulatory and supervisory scrutiny and evolving nature of the risks (e.g. two AML directives in the EU in less than 5 years), and the corresponding increasing investment and importance that financial institutions are giving to their AML/CTF frameworks (connected to the large reputational damage and economic fines of weaknesses in their control model).

3. ***Challenges.*** Financial institutions face a challenging environment when it comes to AML/CTF. The global economy makes tracing money movements ever more difficult. This is made more challenging by the irruption of cryptocurrencies and the proliferation of multitudes of payments technologies. Moreover, local approaches to regulation and legislation, with limited ability to share information and intelligence cross-border have allowed international crime organizations to find weak spots in the system. Those criminal organizations continuously evolve their strategies and build schemas that involve cyberattacks with fraud and money laundering strategies, which financial institutions that still operate in silos find difficult to tackle. Also, the Covid 19 pandemic and the need to use on-line channels and reduce in person contact has made Know Your Customer processes more demanding. Financial institutions need to face those challenges after a sustained environment of low interest rates and severe cost pressure.

4. ***Tailwinds.*** Despite the above, there are tailwinds that financial institutions are using to face those challenges, including the use of technology and data. Advanced automation, BPM (Business Process Management) and robotics are some of the most prominent and help streamline business processes. On the other hand, also relevant is the use of machine learning and AI mechanisms, which help to profile customers and their transactionality in a more efficient way, with a lower number of unproductive alerts or false positives.

5. ***Regulatory environment.*** Regulators are also significantly evolving their frameworks and resources. First by creating supra-national collaboration or supervision bodies, building common databases, performing jurisdiction-wide risk assessments, and strengthening the dialogue and collaboration between Prudential and Non-Prudential supervision. Regulators are also being very active in terms of publication of new policy and guidance on emerging risks that are identified as weaknesses in their supervisory capacity, as well as encouraging firms to use innovation to tackle AML/CTF risks.

6. ***Financial institutions reaction.*** Financial institutions are strengthening their AML/CTF frameworks, through total redesign or specific interventions in their Framework and Governance (including improvements in their Risk Assessment, policies and standards, their split of responsibilities between 1st, 2nd and 3rd lines of defense, as well as their collaboration across sub-risk types). They are also evolving their organisation, giving more hierarchical importance to the head of Financial Crime, performing strategic analysis of future needs, building specialized functions or centralizing capabilities. Other areas of strong

[22]Mohandas Karamchand Gandhi (1869-1948) was the foremost leader of the Indian Independence Movement against the British Raj, practising non-violent civil disobedience, as well as an Indian pacifist, politician, thinker and Hindu lawyer.

focus include their culture and behavior programs, data infrastructure and Management Information, as well as the streamlining and automation of core AML/CTF business processes (KYC, ongoing monitoring, alert management and investigations, down to the engagement with law enforcement and Suspicious Activity Reporting). Finally, the technological infrastructure that underpins the framework is being significantly improved, as is the mathematical capabilities and taxonomy of models.

7. ***Risk Assessment.*** A robust Risk Assessment is at the core of the AML/CTF framework of an organization. Good practices in the industry involve the performance of a risk assessment at different levels, starting with a supra-national and national risk assessments performed by international entities and regulatory authorities, that set the scene of the regional / jurisdiction specific risks associated to AML/CTF. Those inputs inform a business-specific risk assessment of the financial institutions. This will include the identification and assessment of risks associated to the profile of its customer base, products and channels, its scale, geography etc. Finally, the Individual Risk Assessment for each customer relationship takes those as an input and complements with the specific knowledge of the customer, company structure, beneficial owners, sources of funds and wealth.

8. ***Risk Appetite.*** Such comprehensive Risk Assessment informs the Risk Appetite and thresholds to be used when launching new products or services, new business initiatives (e.g. mergers, acquisitions, new business lines etc.). Moreover, it also determines a 'new to bank' score that sets a preliminary expectation regarding customer behavior (type of transactions, channels to be used, etc.), and the risk of AML/CTF associated to the relationship. This is associated to a set of standards around the frequency of periodic review of the relationship, and thresholds for monitoring payments and transactionality that trigger alerts when deviations from the expected behavior take place. Moreover, the more advanced organizations have a regular feedback loop between the incidents identified in their behavioral monitoring and the customer risk assessment, so that the risk profile and associated mitigating actions can be updated immediately.

9. ***Scope of the risk coverage.*** The Risk Assessment needs to cover not only customers, but also third-party suppliers. Financial institutions rely on a number of third parties to execute their day-to-day activities. Depending on the nature of the business, these third parties can also expose the organization to Financial Crime, including AML/CTF as well as Anti-Bribery and Corruption.

10. ***Policies and standards.*** In such a highly regulated environment, it is essential that financial institutions write down and formalize policies, standards and best practices that allow the organization to act under common ways of working and business process. This body of knowledge is also an instrumental mitigating action, since it enables training, awareness, and communication across the organization. Some of the most advanced organizations have a policy architecture in place, with formalized hierarchies of documents that are inter-connected and cross referenced (vertical traceability), published in a digital format that allows easy navigation / browsing, and with quick takeaways, summaries etc. They also have an operating model that ensures ongoing monitoring of new regulation and emerging risks, lessons learned from AML/CTF incidents (internal or in peers) etc. and the timely update of that body of documentation.

11. ***Governance framework.*** One of the aspects that require more investment and strong leadership is the governance framework and three lines of defense (LOD) model for the identification, management, control, and oversight of AML/CTF Risk. It is one of the areas where Regulators and Supervisors have devoted more time and scrutiny. The trend in the industry includes a clear definition and formalization of the role of each of the lines of defense, signed off by the Executive Committee / Board as part of the AML/CTF Risk framework.

12. ***Lines of defense.*** In one of the most widespread archetypes, the first LOD that originates the business and owns the relationship with the client, is also accountable for the risk identification, management, and control of the risk. This includes the deployment of a risk control framework to ensure that the risk profile is kept within appetite, and that the day-to-day operations comply with both internal policies and external regulations. Firms have also reinforced their second line of defense, with the formal appointment of a head of AML/CTF Compliance, or equivalent. In some jurisdictions, this mandatory role needs to be formally approved by the regulator and is expected to have enough seniority to perform independent, effective challenge to the business. Around this role, there are strong compliance and oversight teams that both provide advisory services to the business in basic AML/CTF topics, issues guidance, policies and standards for the adequate identification, monitoring and control of the risks, and oversee the adoption and embedding of those into the business-as-usual activity. The second line of defense in the more mature organizations have a formal AML/CTF oversight plan that involves monitoring of KRIs and KCIs, performance of independent control testing, thematic reviews and more intrusive hands-on investigations of areas that are either in the regulatory radar or for which there are concerns. A fundamental tool of this second line of defense is the Management Information, both in terms of the information itself produced by the business and used as input in the oversight plan, as well as its own independent information that tends to be the one used to report to the Executive Committee and Board / Board delegated Committees. The third LOD, usually lying with the Internal Audit function, evaluates the framework and effective challenge adopted by the second line, as well as the level of adoption of said framework by the first LOD.

13. ***Integration across risks.*** Criminal organizations are becoming increasingly sophisticated in their money laundering schemas; frequently combining cyberattacks (stealing of credentials and impersonation), illicit use of those privileged accesses to commit a Fraud, and using multiple mechanisms to launder the profits of it. As a reaction, financial institutions are evolving their models to an increasingly integrated Financial Crime framework, with a unified Governance model that incorporates all sub-risk types into a single operating model (AML/CTF, Tax Evasion and Fraud, together with Cyber Risk). Although there are different levels of maturity, this usually entails degrees of common risk taxonomy, unified data infrastructure and datasets, joint strategies that try to detect synchronized events of the different risk types or common frameworks for alert analysis and investigations. Some organizations have even centralized the responsibility under a single head and have created centers of excellence that provide operational capabilities across all the sub-risk types.

14. ***Organizational design.*** Even if there is no industry standard around the organizational structure that more effectively implement the three lines of defense model for AML/CTF, both Regulators and financial institutions have a strong expectation that the heads of those teams have reporting lines that allow independent challenge to the business and direct escalation to executive and Board level if needed. Also, that the right seniority and skillsets are present, and that the teams have enough people and technological resource to be effective in their activity. In the second line of defense, the head of AML/CTF oversight tends to report to an executive level, that being Chief Risk Officer, Chief Compliance Officer or Head of Legal / General Council.

15. ***Workforce planning.*** One of the trends and best industry practice consists of connecting the target ambition around AML/CTF, Risk Appetite and strategy, with a strategic planning exercise to assess people's needs in terms of volume, skillsets and expertise, locations etc. Once the analysis is done, there is a tight execution to ensure that such capacity is in place as and when required. This includes training / recycling existing colleagues and hiring new talent (partially nurtured from the bottom, through grads programs, to ensure a continuous supply of subject matter experts irrespective of market conditions).

16. ***Analytical capabilities.*** As part of such a strategic planning exercise, most financial institutions are experiencing a strong demand for analytical capabilities, as many of the underlying AML/CTF processes become more data (and data science) driven - CRA, name screening, transaction monitoring, false positive screening, etc. Most mature organizations are building strong Advanced Analytics teams (in some cases recruiting them from the market, and in other cases repurposing quant profiles from other areas - e.g. prudential risk modelling - to apply their skillsets to new business problems). There are also strong demands for specialized payment profiles, including individuals with detailed technical knowledge of crypto-currencies or, more broadly, new payments technologies. Finally, another profile

that is usually flagged in those exercises are multi-skilled individuals capable of cutting across different disciplines within Financial Crime are also scarce in the market. These are usually profiles that come from a fraud background and also become AML/CTF subject matter experts. These profiles are proving very useful to both refine the detection of joint financial crime strategies, as well as to support multi-purpose centers of excellence that cut across risk types.

17. ***Quality Assurance.*** As organizations become more mature, they tend to create specialized teams to increase effectiveness, cut across different businesses and ensure professionalization of the AML/CTF control activities. Some of those functions include quality control and quality assurance teams, in charge of ensuring that the key business processes where risks can emerge are adequately executed according to policy and procedures. Also specialized second line of defense assurance teams, to support the effective execution of the oversight plan.

18. ***Centers of excellence.*** As part of this specialization, a natural step taken by more advanced institutions has been the creation of centers of excellence. The intention is usually to improve effectiveness and to capture synergies in the execution of operational processes such as customer due diligence (CDD), enhanced due diligence (EDD), name screening, transaction monitoring, payment screening, but also the production of Management Information, or the delivery of continuous improvement and remediation. Some of those financial institutions have found further synergies in incorporating these centers of excellence operational aspects related to Fraud, both internal (employee vetting) and external Fraud. Aspects such as the KYC and onboarding process (e.g. single onboarding team, with the corresponding holistic view of Financial Crime, and simplification of the customer experience), or the development and parameterization of scenarios for AML / Fraud detection etc. are common areas of synergy.

19. ***Regionalization.*** For large International Financial Groups, a natural evolution in their centralization journey has been the regionalization of activities. Namely, the creation of centers of excellence at a regional level, with the corresponding benefits in terms of better management of the pool of resources, removal of duplication, streamlined organizational structure, and better career paths and cross training opportunities for the workforce, with corresponding higher retention rates. In the same line of evolution, some large financial institutions that already operated in off-shore or near-shore countries with lower cost of human resources have been able to build successful centers of excellence in those locations to provide services in the region.

20. ***Outsourcing.*** Finally, whilst outsourcing of some of the operational activities is still an option selected by different financial institutions, there are a number of factors pushing some of those Institutions to have in-house those outsourced capabilities and develop those skillsets within the organization. Not the least of them being an ever-increasing regulatory demand around outsourced activities that are critical to the organization and the associated need to build strong oversight and control structures around the outsourced services, the level of operational excellence expected by the different stakeholders (investors, supervisors, society), and the reputational impact of operational failures.

21. ***Culture and behaviors.*** A key area of investment in strategic AML/CTF programs is the design and embedding of the right culture, ways of working and staff behaviors to combat the underlying financial crime risks. The Supervisory scrutiny is increasing across jurisdictions, and the significant attrition in specialized AML/CTF profiles requires an effective articulation and embedding of the right culture and behaviors to existing and especially new employees.

22. ***Training.*** As part of the AML/CTF cultural programs, financial institutions are investing in strengthening the staff recruitment and vetting processes for staff with responsibilities around AML/CTF. Also, in the development of ambitions training and certification programs (with tight operating models in order to keep the materials updated, measure effectiveness and continuously improve), and that are connected to career progression and remuneration. This also requires a capacity to monitor and measure competences in order to react to deterioration in knowledge and expertise. These programs also invest in the development of clear and transparent messaging from the top (up to Board and Executive level), and strong communication campaigns aimed at different segments of the employee structure, with targeted content for each of them. Finally, Financial institutions are also devoting time to design the right incentives and performance measurement for their workforce, aligned to the Risk Appetite and associated policies.

23. ***Data infrastructure and Management Information.*** In an increasingly data driven economy, one of the key areas of development within the AML/CTF space is the underlying data infrastructure and the Management Information used for decision making. From a Management Information perspective, a market trend is to incorporate, in the Board and executive level reporting, a comprehensive set of metrics and qualitative information to ensure that all the underlying risks (current and emerging) associated to the business are taken into consideration. The MI details the changes in the Risk Assessment at a firm-wide level, as well as a representation of the risks associated to new business relationships (including how many new business relationships per risk category, any new high-risk relationship, any PEP, etc.). For existing relationships, the top management of the organization receives information on the outcomes of the ongoing monitoring activities (e.g. transaction monitoring, payment screening, periodic customer reviews), as well as the summary of the Suspicious Activity Reporting that has taken place, and statistics on positive hits above and below the line. The reporting structure should also contain the exit of existing relationships, and the rationale for those. Finally, it is an advanced practice to incorporate in the MI both open issues coming from the work of Quality Assurance, Internal Audit or Supervisory investigative action, as well as a section on Regulatory Liaison or Industry engagement (usually including an element of horizon scanning for new regulation or legal requirements).

24. ***External information.*** In addition to Management Information, the data landscape and taxonomy underlying the AML/CTF framework is very comprehensive and can be challenging. In addition to client and transactional data generated by the organization, firms rely more than ever on external information (reputed bureaus, national crime agencies, court judgments, public registries of ultimate beneficial owners etc.) to complement their analytical models. This external information, in a number of cases, requires the ingestion, maintenance and comparison against lists to find possible matches of the current or potential clients and transactions. These lists are being enriched with new additions like prohibited digital assets (e.g. virtual currency addresses / digital wallets associated to businesses or individuals under sanctions). Moreover, the adoption of the new messaging standards under ISO20022 will help the screening and comparison of transactions.

25. ***Sanctions and list management.*** Especially in the Sanctions space, list management is a fundamental capability. The most mature firms are implementing a Centralized List Management Platform that aggregates files from different treasury departments and vendors, cleanses the data and then disseminates them amongst all branches according to their local regulations and group's policy, eliminating duplicities and increasing oversight.

26. ***Heterogeneous datasets.*** The nature of the data being captured is also very varied and changing. A standard data taxonomy for AML/CTF can include, in addition to standard transactional information, electronic IDs (e.g. eIDAS in the EU), geolocation, IP addresses or even IMEI and device model of the devices used in convertible virtual currency transactions. Also lists containing non-trusted IP addresses, IP addresses from sanctioned jurisdictions or IP addresses flagged as suspicious. Moreover, adverse media files and information from social media can include audio or video format, which highlights demand for unstructured information and the corresponding underlying infrastructure to store and exploit it.

27. ***Data management capabilities.*** These demands on data require the development of Data Management capabilities. One of them is a Data Quality capability to proactively specify business rules and data quality standards around critical data, and then systematically measure those rules to identify any breaches. Also, a Data Catalog that allows harmonization of data across different repositories and engines. Finally, Financial institutions are investing heavily in data lineage capabilities to enable end-to-end traceability of the data from the point of consumption back to the point of origination.

28. ***Harmonization of data infrastructure.*** One of the most important principles in terms of data infrastructure has been the convergence to single data repositories so that all the technological components or business processes involved in the AML/CTF framework feed data from and store data back to the repository, making it available immediately to the rest of components. This centralization can happen regionally or even group wide. In order to gain a holistic view of the customer risk and standardize alert investigation and reporting, it is indispensable to consolidate KYC, Screening, Transaction Monitoring, and Alert & Case Management data into a single platform. Consolidating basic information required for an investigation before the alert is assigned enhances the time per alert plus automatic notifications to the Compliance department when an alert is pending authorization.

29. ***Business processes – Client onboarding.*** In relation to business processes to onboard new clients and associated KYC, the evolution of customer behaviors, accelerated by the Covid 19 pandemic, has fueled the dominance of the digital channels in financial interactions. Institutions are investing in automated self-servicing solutions through digital channels, actionable by the user, using a Digital ID and Biometric data, to empower customers during the onboarding process, periodic reviews and recertification. Moreover, it allows for more targeted, risk-specific information gathering (at onboarding or whenever there is a trigger), with dynamic questionnaires aligned to a predefined segmentation. These processes now connect directly, through APIs and microservices, to external sources of data in order to retrieve them automatically and therefore simplifying the customer experience, whilst independently validating customer inputs. These solutions also ease automated record keeping of customer support during due diligence process, which can be instrumental in a potential investigation process.

30. ***Business processes – Transaction Monitoring.*** Another process that financial institutions are drastically improving is Transaction Monitoring. It is very demanding from a data and computational perspective in order to calculate the likelihood of each scenario. Financial institutions are investing in technology with higher computational capacity, leveraging on cloud computing. Moreover, they are refining the execution of scenarios based on customer segmentation (instead of running all scenarios for all the data available, scenarios are customized to adapt to the Institution's risk profile and business reality in terms of geography, product catalogue, etc.). Another option to increase efficiency is to perform simulations (number of alerts, false positives, false negatives, etc.) in a sandbox environment before deploying the scenario into Production or running scenarios only against susceptible customers, omitting, for instance, government and public agencies with very low risk. Some institutions run retroactive batch screening to identify potential links with sanctioned entities and flagging those customers as high-risk individuals to be investigated.

31. ***Business processes – Real time assessment.*** In terms of scanning customer's data (identification data during onboarding, or transactions during normal business), the market trend is that these run-in real time. Therefore, there are strict demands on SLAs for list maintenance, and a technical process that ensures that the online checks are not impacted by the batch reprocessing of the back book of all customer records whenever a list is updated. Moreover, the digital footprint is a rising method for identification of red flags in payment screening. In the more advanced organizations, the IP addresses collected during customer's operations, associated with transactions and logins, is routinely monitored and compared with the ones ingested during onboarding to detect misuse of an account from a High-risk/Sanctioned country or account theft. The detection of Tor associated IP addresses (that anonimises web traffic) is fundamental, as it might reveal connections between the customer and criminals from the darknet.

32. ***Business processes – Reporting.*** Even when risk detection is successfully implemented, poor reporting could tamper the process. Financial institutions are improving their processes to ensure that their local FIU's expected SLAs are met, and that changes to the reporting formats and requirements are incorporated swiftly. Moreover, there are automation opportunities in the execution of regulatory steps that do not require manual intervention. Finally, the communication channels between AML/CTF functions and the lines of business must be very dynamic, to ensure that the answers to questions or gathering of further information is performed within Regulatory deadlines.

33. ***Machine learning.*** As discussed, real time detection technologies are being broadly adopted to prevent risks associated with unnoticed errors and improve customer experience. For transactional and name screening (or cases outside AML/CTF, like Fraud audio detection) the more advanced institutions are investing in machine learning libraries for Natural Language Processing (NLP) in order to collect, analyse and store audio information and create alerts to the lines of business interacting with the customer, finalizing the call immediately to avoid sharing any personal information.

34. ***Technological infrastructure.*** From a technological infrastructure perspective, AML/CTF tooling landscape can no longer rely only on a relational DataMart as a central database, as it is now receives unstructured data (image, audio, video…) where NoSQL and Data Lakes become more effective.

35. ***Distribute ledger technology.*** Technological advances are also enhancing list management systems, moving from classical list management systems administering tables and files to Distributed Ledger Technology (DLT). DLT helps safeguard data integrity, traceability, confidentiality, encryption and agreement between responsible stakeholders. Additionally, it allows regulators to audit the transaction book, containing the sequence of timestamped changes in the list) to validate compliance.

36. ***Advanced Robotics.*** Another technological trend that firms have been using to gain efficiency and improve effectiveness is advanced Robotic Process Automation (RPA). Virtual agents, chat-bots and call-bots can assist customers with structured and repetitive inquiries day and night without interruption, getting them in contact with a human resource for queries that are more complex. RPA is also a crucial improvement for Alert and Case Management, as these algorithms can ingest more data from more sources quicker than a human investigator, enabling faster analysis of a broader evidence base and, ultimately, more accurate resolution. More sophisticated systems will automate steps or results based on previous investigations and outcomes.

37. ***End to end improvements.*** All these technological improvements combined allows for machine learning models to be used to score alerts, in order to discriminate potential false positives. Compliance department should have established a clearly defined and objective workflow for the review of alerts, with a prioritization criterion to analyze alerts (for example, based on risk profiles, transaction amount or matching scores). This process is only possible if carried by specialized AML teams to handle the sleuth of complex organizations and manage whitelists.

Financial Crime Risk definition and regulatory context

"The criminal element now calculates that crime really does pay"
Ronald Reagan[23]

Financial Crime refers to illegal acts committed by an individual or group of individuals to obtain personal financial gain utilizing the means of financial services or financial markets. Although there are different definitions of what Financial Crime entitles[24], under this concept the actions of ML/TF, bribery, market abuse, or fraud are considered[25].

Two definitions of Financial Crime from FCA and FDIC are highlighted:

> *"Any kind of criminal conduct relating to money or to financial services or markets, including any offence involving: (a) fraud or dishonesty; or (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime; or (d) the financing of terrorism"*[26]

> *"Legal entities can be abused to disguise involvement in terrorist financing, money laundering, tax evasion, corruption, fraud, and other financial crimes"*[27]

Creating the means to identify and prosecute illicit financial crimes in their different forms have triggered the enactment of different supervisory and regulatory initiatives. The two critical actions promoting greater global coordination on ML regulation were the constitution of the Financial Action Task Force (FATF)[28] and the UN's ratification of the Convention on Transnational Organized Crime[29], the first AML treaty. As part of the FATF, the Member States are required to comply with global AML standards. These standards[30] broadly define the core components of any modern AML program at any financial institution:

- Implement Know Your Customer (KYC) ID verification measures.
- Perform FATF recommended due diligence measures.
- Maintain suitable records of high-risk clients.
- Regularly monitor accounts for suspicious financial activity and report that activity to the appropriate national authority.
- Enforce effective sanctions against legal persons and obliged entities that fail to comply with FATF regulations.

On the other hand, the FATF's principles and the UN's Convention agreements created a consensus to start working on the identification of ML/TF practices, and more importantly, to stop them.

During the last decades, the concept of AML has evolved differently, as well as the various regulations, depending among other things on the changing nature of CTF financial activities. Key trends noted in international Financial Crime activities include:

- Tight restrictions on transactions in most jurisdictions, which increases the appetite of financial criminals to divert to other types of activities such as crypto and digital currency in incipient stages of control and regulation.
- Customer attitudes, preferences and behaviour changing, with increasing focus on digital banking services[31], which will be the target of financial criminals (e.g., virtual assets, custodian wallets, fiat currencies, pre-paid cards).

[23] Ronald Wilson Reagan (1911-2004) was an American actor, statesman and politician who served as the 40th President of the United States (1981-1989) and 33rd Governor of California (1967-1975).

[24] Some regulatory or supervisory bodies, such as FCA, provide "closed" definition of the term "financial crime" and the actions considered within, whilst others may claim responsibility for assessing, regulating and supervising certain illegal acts that might qualify as financial crime (e.g., FINCEN). The identified actions of ML and TF are nevertheless core to any financial crime supervisory program.

[25] Other illegal acts with financial gains implied that are subject to overall regulation include: identity theft, corruption, tax evasion, embezzlement, forgery, counterfeiting.

[26] Financial Conduct Authority (2021).

[27] Appendix A to § 1010.230—Certification regarding beneficial owners of legal entity customers , FDIC Law, Regulations, Related Acts.

[28] FATF (2019).

[29] UN Office on Drugs and Crime (2005).

[30] Despite the complexity of the topic and the constant evolution of the ML tactics and available technology for it, these standards remain at the core of the AML programs worldwide and address AML evaluation requirements: customer risk rating assessment, transaction monitoring program and sanction screening program. Standards relating to high-risk customers are especially important, as the risk-based approach is quintessential to the definition of any AML program.

[31] This trend has been exacerbated as a result of the COVID19 pandemic.

- Increased international financial activities facilitated by available technologies has fostered new global consumption requirements, which creates new channels for illicit financial activities.

The complexity of the current environment is forcing the regulatory authorities to take action and address the modernization of the Financial Crime programs in light of these transformative elements.

Regulatory changes for 2021 and 2022 that pertain to Financial Crime are expected to focus on:

- Stricter restrictions to prevent ML in "non-traditional" circuits, e.g., new rules for digital transactions.
- Increasing focus on the foundations of the KYC program to monitor customer risks and to therefore reinforce the AML regulation.
- Introduction of new technologies and analytics (e.g., cloud services, machine learning / artificial intelligence model, advanced analytics) to move to real-time identification and optimized resources use.
- Coordination across jurisdictions to improve Financial Crime programs.
- Public and private cooperation and development of platform for sharing information.

One of the most important regulatory trends has been the strengthening of interbank and inter-jurisdiction collaboration with the aim of increasing the capabilities of data sharing and information on financial crimes and creating homogenous rules that could act in coordination[32]. Although these initiatives are in the earliest stages, they are proving successful (as has been seen, for example, in the reaction of different regions to the Russia invasion of Ukraine, and the corresponding sanctions imposed on Russian economic interests).

Regulatory landscape across different jurisdictions

The United States have been developing regulation in this regard since 1970. However, in recent years new regulation has been issued to update the existing corpus:

- The AML Act of 2020[33] modernized the Act of 1970 (BSA/AML) incorporating critical elements to address ML and fraud issues in alignment with the current trends.
- Same regulation acted on the requirements for Ultimate Beneficial Owners. Banks will have better visibility on the ultimate beneficiary of a transaction, which will enact reinforced customer due diligence (CDD) and reduce ML and fraud activities.
- Cryptocurrency exchanges should complete the KYC process for each customer[34].

In the case of the European Union, the EC presented a package with four legislative proposals related to AML/CTF[35]. The objective of this new legislative package is to address the differences in national regulations and increase coordination among member states.

The UK government is actively working to comply with international AML standards and considering the introduction of national priorities into the AML Act[36]. The government is progressing its 2019-2022 Economic Crime Plan[37] to strengthen Financial Crime frameworks. In its latest statement of progress on this Plan, several core actions were developed that build on the original actions within the Economic Crime Plan[38,39].

In China, CBIRC issued new measures[40] to encourage financial institutions to effectively fulfill their AML/CTF obligations and regulate the supervision and administration of AML/CTF.

Japan has recently issued AML/CTF guidelines[41] that also prescribe a risk-based approach that complies with international standards, such as the FATF.

In Singapore, the Payment Services Act[42] was updated in January 2021. This regulation provides a flexible framework for payment systems and payment service providers in the country. Recently the Monetary Authority of Singapore (MAS) also published two consultation papers that seek to strengthen the regulatory framework surrounding money laundering[43].

[32] FATF included in their agenda the public private partnership (PPP) initiative. Different regulators have also launched similar initiatives.
[33] FinCEN.gov (2020).
[34] Apart from this important addition to the KYC rules, other regulations on virtual assets were issued by the U.S. Securities and Exchange Commission, Commodity Futures Trading Commission and FinCEN to reinforce the framework of control of these assets in the US.
[35] Regulation to establish an EU AML/CTF authority; Regulation for applicable AML/CTF rules (Single Rulebook) and entities subject to them; Directive 6 on AML/CTF (AMLD6) replacing previous one, to be transposed into national law with rules for national supervisors and FIUs in Member States and Regulation on Transfers of Funds
[36] The Institute of International Finance and Deloitte (2021).
[37] HM Government (2019).
[38] HM Government (2021).
[39] i) Design and deliver a comprehensive Fraud Action Plan; ii) Bolster public-private operational action to tackle known vulnerabilities enabling the flow of illicit finance within and out of the UK; iii) Improve the effectiveness and efficiency of the whole system response to economic crime, increasing high value intelligence to law enforcement and reducing low value activity that costs business and delivers little benefit; iv) Continue to deliver SARs reform, including the next stages of rollout of the new IT infrastructure and the increase in UK Financial Intelligence Unit staffing; v) Finalize the Sustainable Resourcing Model to support economic crime reform, vi) Develop legislative proposals to tackle fraud, ML, seize more criminal assets, and to strengthen corporate transparency and vii) Capitalize on the G7 Presidency to strengthen the overall international response to illicit finance and anti-corruption.
[40] Institutions. People's Bank of China (2020).
[41] Financial Services Agency (2021).
[42] Republic of Singapore (2019).
[43] See: Consultation Paper on Proposed AML Notices for Cross-Border Business Arrangements of Capital Markets Intermediaries under Proposed Exemption Frameworks. Monetary Authority of Singapore. May 12, 2021, and Consultation Paper on the FI-FI Information Sharing Platform for AML/CTF. Monetary Authority of Singapore. October 2021.

The following list contains the main supervisory and regulatory bodies acting on the Financial Crime program implementation and the core regulations and guidelines. The historical evolution explains the major focus on AML/CTF.

United States – Regulatory Body: FinCEN

- *Bank Secrecy Act (BSA), Currency and Foreign Transactions Reporting Act of 1970* | 26-Oct-70. Defines the regulatory framework for U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering, including transactions exceeding $10,000, report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.

- *Title III USA PATRIOT Act of 2001* | 26-Oct-01. Section 314 helps identification, disruption and prevention of terrorist act and money laundering activities.

- *Corporate Transparency Act of 2019* | 11-Jun-19. Requires new and existing entities to report beneficial ownership information to the Financial Crimes Enforcement Network ("FinCEN"), creates a beneficial ownership database, and institutes civil penalties, fines, and criminal sanctions for noncompliance.

- *AML Act of 2020 (US AMLA)* |1-Jan-21. Requires FinCEN to establish national AML/CTF priorities for FIs to incorporate them into their AML/CTF programs, and collect and report additional information on account holders, including information on ownership and control. It also requires regulators and examiners to incorporate into rules, guidance, and examinations.

- *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* | 30-Jun-21. Government-wide priorities for anti-money laundering and countering the financing of terrorism.

United Kingdom - Regulatory Body: UK Gov't

- *Proceeds of Crime Act 2002* | 24-Jul-02. Established the Assets Recovery Agency and made provision about the appointment of its Director and his functions (including Revenue functions) and sets out the legislative scheme for the recovery of criminal assets.

- *Criminal Finances Act 2017* | 27-Apr-17. An Act to amend the Proceeds of Crime Act 2002; make provision in connection with terrorist property; create corporate offences for cases where a person associated with a body corporate or partnership facilitates the commission by another person of a tax evasion offence; and for connected purposes.

- *The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017* | 28-Jun-17. The Treasury are designated for the purposes of section 2(2) of the European Communities Act 1972 in relation to the prevention of money laundering and terrorist financing.

United Kingdom - Regulatory Body: FCA

- *Financial Services Act of 2012* | 19-Dec-12. An Act to amend the Bank of England Act 1998, the Financial Services and Markets Act 2000 and the Banking Act 2009; to make other provision about financial services and markets; to make provision about the exercise of certain statutory functions relating to building societies, friendly societies and other mutual societies; to amend section 785 of the Companies Act 2006; to make provision enabling the Director of Savings to provide services to other public bodies; and for connected purposes.

United Kingdom - Regulatory Body: JMLSG

- *Guidance for AML and combating terrorism finance* |20-Dec-21. Sets out what is expected of firms and their staff in relation to the prevention of money laundering and terrorist financing but allows them some discretion as to how they apply the requirements of the UK AML/CTF regime in the particular circumstances of the firm, and its products, services, transactions and customers.

European Union - Regulatory Body: EC

- *Anti-Money Laundering Directive* | 9-Jun-18. Set out factors that firms should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction. In addition, they provide guidance on how financial institutions can adjust their customer due diligence measures to mitigate the ML/TF risk they have identified so as to make them more appropriate and proportionate. Finally, they support competent authorities' AML/CTF supervision efforts when assessing the adequacy of firms' risk assessments and AML/CTF policies and procedures.

- *Commission Delegated Regulation (EU) 2019/758* | 31-Jan-19. Regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries.

- *Proposal for a 6th Directive on AML/CTF (AMLD 6)* | 20-Jul-21. Directive on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849.

- *Anti-money laundering and countering the financing of terrorism legislative package* | 20-Jul-21. The package includes a proposal for the creation of a new EU authority to fight money laundering. It is part of the Commission's commitment to protect EU citizens and the EU's financial system from money laundering and terrorist financing. The aim is to improve the detection of suspicious transactions and activities, and close loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system.

European Union - Regulatory Body: EBA

- *Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CTF Compliance Officer* | 14-Jun-22. The guidelines comprehensively address, for the first time at the level of the EU, the whole AML/CTF governance set-up. These guidelines specify the role, tasks and responsibilities of the AML/CTF compliance officer, the management body and senior manager in charge of AML/CTF compliance as well as internal policies, controls and procedures. They complement, but do not replace, relevant guidelines issued by the European Supervisory Authorities on wider governance arrangements and suitability checks.

European Union - Regulatory Body: ESMA

- *2020 Annual Report on the EU Market Abuse Sanctions* | 20-Oct-21. The Report describes an increase in the number of administrative sanctions and measures in 2020 compared to 2019, reaching 541 from 279 the preceding year. However, it also found that the financial penalties imposed are significantly lower, reaching only €17.5 million in 2020, compared to €82 million in 2019.

- *Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing* | 13-May-20. In its Communication Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework and accompanying reports of July 2019, the Commission set out the measures needed to ensure a comprehensive EU policy on preventing money laundering and countering the financing of terrorism (AML/CTF). These include better implementation of existing rules, a more detailed and harmonized rulebook, high-quality and consistent supervision,

including by conferring specific supervisory tasks to an EU body, interconnection of centralized bank account registries and a stronger mechanism to coordinate and support the work of the Financial Intelligence Units (FIUs).

China - Regulatory Body: BIRC

- *Measures for the Supervision and Administration of Anti-Money Laundering and Counter-Terrorist Financing of financial institutions* | 1-Aug-21. In order to cause financial institutions to effectively fulfill their anti-money laundering and anti-terrorist financing obligations and regulate the supervision and administration of anti-money laundering and anti-terrorist financing, the People's Bank of China formulated the Measures for the Supervision and Administration of Anti-Money Laundering and Anti-Terrorist Financing (the "Measures") in accordance with the Anti-Money Laundering Law of the People's Republic of China, the Banking Law of the People's Republic of China and the Anti-Terrorism Law of the People's Republic of China.

Japan - Regulatory Body: FSA

- *Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism* | 19-Feb-21: The Financial Services Agency ("FSA"), with necessary supervisory measures, shall monitor the AML/CTF measures of each Financial Institution, share the outcome with financial institutions, and urge them to enhance risk management. The Guidelines clarify the required actions and expected actions to be implemented by each Financial Institution and how the FSA shall conduct monitoring going forward.

India - Regulatory Body: FIU

- *Prevention of Money Laundering Act* | 17-Jan-03. An Act of the Parliament of India enacted by the NDA government to prevent money-laundering and to provide for confiscation of property derived from money-laundering.

Australia - Regulatory Body: AUSTRAC

- *Financial Transaction Reports Act 1988* | 16-Apr-18. The FTR Act was introduced to assist in administering and enforcing taxation laws as well as other Commonwealth, state and territory legislation.

- *Anti-Money Laundering and Counter-Terrorism Financing Act* | 12-Dec-06. Provides for measures to detect, deter and disrupt money laundering, the financing of terrorism, and other serious financial crimes; and provides relevant Australian government bodies and their international counterparts with the information they need to investigate and prosecute money laundering offences, offences constituted by the financing of terrorism, and other serious crimes.

South Africa - Regulatory Body: FIC

- *Financial Intelligence Centre Act* | 28-Mar-03. Establishes the country's Financial Intelligence Centre (FIC) and introducing a basic framework to bring the country's AML/CTF regulations into alignment with those of the wider international community. This act was strengthened by the Financial Intelligence Centre Amendment Act 1 of 2017, introducing a risk-based approach to customer due diligence.

Global - Regulatory Body: UN

- *Convention against Transnational Organized Crime and the Protocols Thereto* | 15-Nov-00. The purpose of this Convention is to promote cooperation to prevent and combat transnational organized crime more effectively.

Global - Regulatory Body: OECD

- *International Co-operation* | 14-Jun-12. This OECD report contains a compilation of a variety of international regulations on financial crime.

- *Against Tax Crimes and Other Financial Crimes* | 14-Jun-12. This OECD report contains a compilation of a variety of international regulations on financial crime.

Global - Regulatory Body: FATF

- *FATF Recommendations 2012* | Oct-21.The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats.

- *FATF Methodology 2013* | *Nov-20.* The FATF conducts mutual evaluations of its members' levels of implementation of the FATF Recommendations on an ongoing basis. These are peer reviews, where members from different countries assess another country. The FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CTF systems sets out the evaluation process.

- *Procedures for the FATF Fourth Round of AML/CTF Mutual Evaluations* | Jan-21. The FATF is conducting a fourth round of mutual evaluations for its members based on the FATF Recommendations (2012), and the Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CTF Systems (2013), as amended from time to time. This document sets out the procedures that are the basis for that fourth round of mutual evaluations.

- *Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up* | Jan-21. The Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up set out the core elements that form the basis for all evaluations and are based on the Procedures for the FATF 4th Round of AML/CTF evaluations.

Global - Regulatory Body: BCBS

- *Core Principles for Effective Banking Supervision* | Oct-06. The Core Principles have been used by countries as a benchmark for assessing the quality of their supervisory systems and for identifying future work to be done to achieve a baseline level of sound supervisory practices.

- *Guidelines on the Prudential Management of Risks Related to Money Laundering and Terrorist Financing (AML/CTF)* | Jul-20. These guidelines are intended to enhance the effectiveness of the supervision of banks' money laundering and terrorist financing (TF) risk management, consistent with and complementary to the goals and objectives of the standards issued by the Financial Action Task Force (FATF) and the principles and guidelines issued by the Basel Committee.

- *Updated guidelines for a risk-based approach to virtual assets and virtual asset service providers* | Oct-21. The Financial Action Task Force (FATF) published in October 2021 a set of guidelines setting out how the FATF recommendations should be applied in the context of distributed accounting technology and cryptocurrencies.

Challenges and trends in anti-money laundering and counter terrorist financing

"Business must harness the power of ethics which is assuming a new level of importance and power."
James Joseph[44]

There is a set of capabilities that can be considered under an AML/CTF map for financial institutions, which are intended to allow the identification, management, control, and oversight of ML/TF. This map includes (i) the framework and governance; (ii) the organizational structure; (iii) the business processes (including KYC, customer risk assessment, sanction screening, as well as transaction monitoring or payment screening, amongst others); (iv) the technological infrastructure; and (v) the data infrastructure and analytics capabilities (see figure 1).

Framework and Governance

At the foundation of their AML/CTF programs, financial institutions are enhancing their risk framework and governance models, to ensure both a comprehensive scope, as well as an effective embedding into the business. To this end, the framework includes the process of risk assessment, setting standards and policies, and ensuring robust risk management through a three Lines of Defense model.

Risk assessment

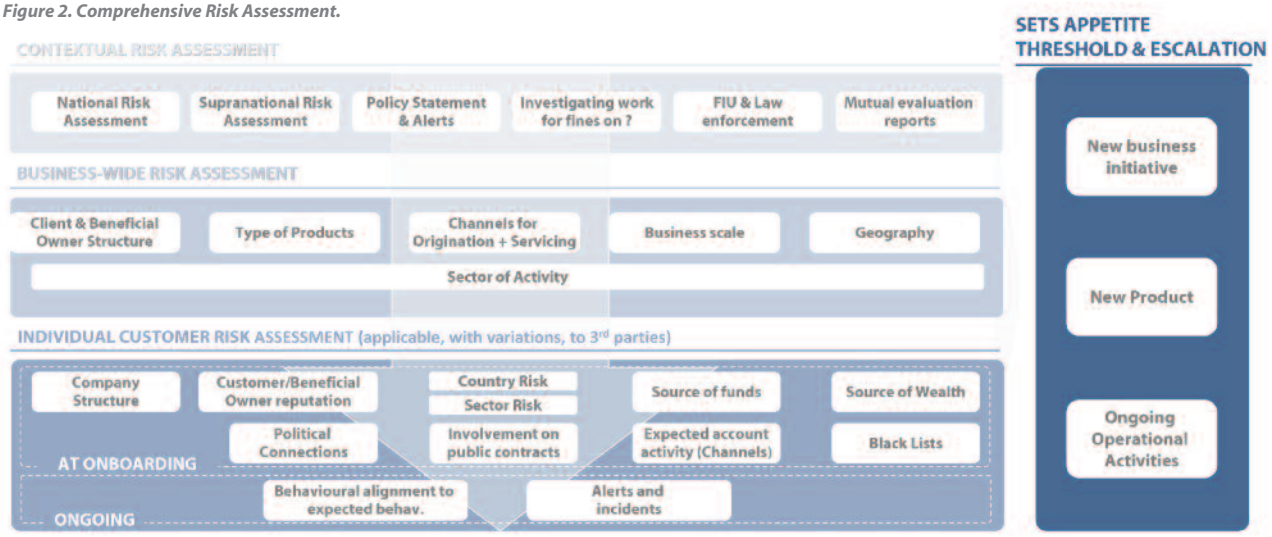
The Risk Assessment is a mechanism to understand the sources of risk, and it is one of the central components of the approach of a firm to AML/CTF.

The process of risk assessment has four main components that can be implemented: contextual, business-wide, customer and third-party risk assessment.

[44] James Joseph Sylvester (1814-1897) was an English mathematician who made important contributions to the field of matrices (he coined the terms matrix, invariant, discriminant and others), as well as to the theory of algebraic invariants (in collaboration with A. Cayley), determinants, number theory, partitions and combinatorics.

Figure 1. Generic map of AML/CTF capabilities in an advanced financial institution.

Figure 2. Comprehensive Risk Assessment.



Contextual Risk Assessment

The starting point of the Risk Assessment is a comprehensive review of the business model, as well as the context in which such business is conducted. There are many drivers for this analysis (see figure 2). In addition, an important input to this process is the regional / local Risk Assessment provided by the corresponding regulatory authority. In many countries, the supervisory authority has the mandate to perform a comprehensive Risk Assessment on AML/CTF[45,46,47].

Business-wide Risk Assessment

The business-wide Risk Assessment is the mechanism that enables financial institutions to assess, for each part of its business and within it[48]), where the major risks are.

Moreover, the business-wide Risk Assessment provides the framework and context in which to assess the AML/CTF risks in new product design as well as in individual business relationships, enabling a comprehensive review of the relationship through the different risk factors that impact the business.

Setting up a formal process, involving the right subject matter experts in the business, and ensuring that the risk assessment is reviewed on a continuous basis are some of the industry practices in advanced firms[49].

Customer Risk Assessment

At the most granular level, financial institutions perform individual Customer Risk Assessments (CRAs) to analyze the arising risks at the point of onboarding of a new client, as well as throughout the lifecycle of the client. This assessment shall include a minimum set of factors, which regulators have provided (e.g. sources of wealth and funds or specific country and sector risk factors)[50,51].

Historically, the data and mathematical capabilities devoted to CRA have been limited, triggering customer classifications that did not always discriminate high-risk clients, or that inadequately classified large number of customers into medium or high-risk buckets, with the corresponding operational effort required on monitoring, and the impact on customer experience.

As a result, financial institutions have devoted significant investment to get a more accurate risk-based approach and risk management. Currently, the efforts are focused on simplifying the taxonomy of models aligning to a common set of families of variables (e.g., Customer, Transaction, Channel, Product, Region), that are used consistently across the organization, to ensure completeness and adequate discrimination[52].

[45] See, for example, Article 6(5) of (EU) 2015/849 (The Fourth EU Anti-Money Laundering Directive), which requires the EBA to issue an Opinion on the risks of ML and TF affecting the EU's financial sector every two years.

[46] See the 'Opinion on the risks of money laundering and terrorist financing affecting the European Union's financial sector'.

[47] FATF (2013). https://www.fatf-gafi.org/documents/documents/nationalmoneylaunderingandterroristfinancingriskassessment.html

[48] It depends on its sector risk, business scale, customer and beneficial owner profiles and structure, the product types and complexity, channels used for distribution or servicing, transactions, and geographies.

[49] This process allows to formally include AML/CTF in the Risk Appetite framework, since it drives the operational activities in the business and strategic decisions in the new products approval committees, new business initiatives (like mergers, acquisitions, etc.) and new transformation projects.

[50] EBA (2017a) https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

[51] FCA (2022). https://www.handbook.fca.org.uk/handbook/FCG.pdf

[52] The more advanced financial institutions already use machine learning algorithms and behavioral models to assess the customer risk. These algorithms are trained and calibrated with historical data and, when required, with expert judgment, with significant improvements in accuracy versus traditional models which primarily consider expert judgment.

Third party Risk Assessment

Finally, some financial institutions rely on third parties to execute part of their day-to-day activities, from brokers and intermediaries to outsourcing operational activities, the provision of training, advisory, technological infrastructure services, etc. Depending on the nature of the business, these third parties can also expose the organization to AML/CTF[53] (or other forms of Financial Crime).

Therefore, it is common practice to have a fully integrated approach to third party vendor risk management to assess the underlying ML/TF risks. To this end, procurement teams undertake specific training to be able to act as a 'first line of defense' and perform the comprehensive assessment.

Standards and policies

A comprehensive body of documentation that specifies the standards to be followed across the organization is one of the strategic pillars of any AML/CTF framework, and one of the most effective mechanisms to mitigate the risk.

The most advanced organizations have the following elements in place:

- A policy architecture that, starting from a framework of documentation, progressively cascades down into business specific standards, as well as procedures and guidance instructions[54].
- Adequate mechanisms to effectively communicate and embed those policies into the actual BAU activity of the organization. These can include the existence of a web portal where the documentation is accessible to the relevant employees, together with a comprehensive training and awareness program and effective communication process to ensure that any relevant addition or change to the policy landscape is immediately communicated across the organization).
- Well-established operating model that enables policies to be reviewed and updated regularly, so that new regulation and emerging risks in the business, or lessons learned from AML/CTF incidents, are adequately and timely updated in the documents, and communicated across the organisation. Senior Management should drive this update, and the effective integration of the policies in the business processes[55].

The three lines of defense model

As with other risks, a robust three lines of defense (LOD) model is one of the pillars of the AML/CTF management framework, since it establishes the responsibilities for the identification, management, control and oversight of the underlying risks.

Financial institutions have reinforced their lines of defense model by performing a more granular split of responsibilities and accountabilities between them.

[53] EBA (2017b). https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

[54] Each document contains references to the risks it refers to (connected to the Risk Assessment when applicable), as well as to the external references (regulation and legislation, industry guidance etc.) that allows compliance and traceability.

[55] EBA (2017c). https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

First line of defense

The first line of defense is ultimately responsible for the identification, management and control of the risks originated in the conduct of business, as well as being in compliance against internal and external regulation. It maintains the relationship with the client, which involves carrying out basic KYC activities[56], and monitoring of the risk profile[57]. It is also responsible for deciding and coordinating customer exits.

In order to ensure the professionalization and standardization in the ways of working, and adequate resourcing, the more advanced institutions have formalized the role of an AML/CTF function or unit in the business that supports the business teams in the exercise of their accountabilities (see section on Organizational Structure).

Second line of defense

The second line of defense is in charge of setting up the AML/CTF framework, issuing policies (to adapt external regulation to the internal reality of the business) and eventually oversee their adequate implementation. In most financial institution, there tends to be also an element of advisory to the first line in complex cases of customer onboarding and exits, as well as in the case of new product / service development, etc.

In advanced financial institutions, the second LOD develop a formal oversight plan with different actions which combines the input obtained from different sources with the specialized knowledge about the business and firm-wide risk assessment or areas of regulatory concern. The action within the plan might include the issuance of new policy or guidance, more frequent management information of particular topics, increased sampling of cases, or more 'intrusive' thematic reviews and specialized on-site inspections.

The second LOD also produces regular management information and reporting to the internal governing bodies, to keep them informed of the evolution of the risk profile of the organization and any relevant point for escalation (e.g., gaps in the control environment, new high-risk relationships etc.).

The Head of AML/CTF oversight usually reports to an executive level: Chief Risk Officer, Chief Compliance Officer or Head of Legal / General Council, or in its case, a member of the Board of Directors[58] or within the Senior Management. Such nominated officer[59] is an individual with ultimate responsibility for the oversight of the framework and all the activity associated to AML/CTF. This individual and their team act as the central point of reference for both independent and effective challenge, as well as for advisory on specific, complex topics.

Third line of defense

The third LOD usually lies with the Internal Audit function of the organization. As with the rest of risks, this is an independent function from the business and the risk organization, reporting directly to the Board Audit Committee. Their responsibilities are to evaluate and assess the comprehensives and effectiveness of the framework defined by the second line of defense, its level of adoption by the first LOD and the level of independent oversight and effective challenge that the 2nd LOD performs.

The 3rd LOD has its own, independent audit plan that receives the 1st LOD and 2nd LOD management information as input and develops its own set of audits.

Organizational Structure

Specialized functions

In the last decade, financial institutions have been under intense pressure to reduce costs, given the sustained period of low interest rates to which they have been subjected, and the added financial impact of the pandemic. At the same time, they have been expected to improve the effectiveness and efficiency of their operations to increase the number of productive alerts and detection of ML attempts.

In terms of effectiveness, there is a trend to further professionalize certain functions within the AML/CTF function. Some examples include:

1. The creation of specialised teams of Quality Control / Quality Assurance in the first line of defence, which use a full set of techniques to perform advanced sampling in order to identify failures in the compliance against policies and procedures and raise recommendations for improvement.

2. The creation of specific Assurance and Oversight functions in the second line of defence. In line with the discussion

[56] For example, customer information gathering, identification and validation, CDD (or Enhanced Due Diligence, when required) and Customer Risk Assessment.

[57] This includes the ongoing monitoring of transactions (using in general advanced models to detect outlier behaviour and well-known money laundering strategies), screening of payments against watchlists, etc. As in the case of the onboarding, the analysis and clearance of low-level alerts tends to happen in the business as well, and escalation to the second line of defines happens only in those cases of suspected true positives.

[58] In certain jurisdictions it is required that the institution formally designate a member of the Board of Directors or within the Senior Management as the officer ultimately responsible for compliance with the regulation. See, for example, EBA Guidelines on the role of AML/CTF compliance officers, EBA/CP/2021/31. See also The Financial Conduct Authority ML 7.1 The money laundering reporting officer.

[59] Nominated officer is not necessarily considered a formal role. For example, in the UK regulation, it recognizes the role of a nominated officer', as does the role of a Money Laundering Reporting Officer (both roles can be put onto the same individual, see Financial Conduct Authority Handbook).

.

above, these teams act as a layer of execution of the oversight plan and performs deep dives in the form of detailed, specialised revision work on specific subject matters.

3. The creation of AML/CTF analytics teams. They tend to incorporate other sub-risks in addition to AML/CTF. (e.g., fraud) and are usually very business-oriented teams, identifying any new trend in the market.

4. The creation of specialised capabilities around change and remediation in the business. The combined effect of the multiple layers of control and oversight translate into a portfolio of recommendations, issued from the Quality Control teams, Internal Audit teams and Supervisory reviews.

Centralization and the creation of centers of excellence

In connection with the drive for more efficient operations, a number of large financial institutions have pulled the lever of centralisation of some of the operational activities within their AML/CTF teams, creating centres of excellence. Some of the operational activities that have been centralised include the Customer Due Diligence, which incorporate the checks and controls around KYC, and the performance of the Customer Risk Assessment, etc[60]. These teams usually have a specialization by Retail and Corporate, to account for the differences in the KYC / KYB processes. Some Institutions have a specialized team in KYS (Know your Supplier), and perform the AML/CTF as well as the Fraud and ABC assessment of their Suppliers in a single team.

For large International Financial Groups, a natural evolution in their centralization journey has been the regionalization of activities (i.e., the creation of centers of excellence at a regional level) with the corresponding benefits in terms of better management of the pool of resources, removal of duplication, streamlined organizational structure and better career paths and cross training opportunities for the workforce.

Although outsourcing some of the operational activities is an option, there are a number of factors pushing some financial institutions to on-board back the outsourced capabilities and develop the skillsets within the organization. Some of the factors are the increasing regulatory demand around outsourced activities that are critical to the organization, the associated need to build strong oversight and control structures around the outsourced services, the level of operational excellence expected by the different stakeholders, or the reputational impact of operational failures.

[60]There are further examples such: the execution of name screening and associated maintenance of watchlists; the performance of Transaction Monitoring (as in the case of CDD, with a natural split between Retail and Corporate); the execution of Payment Screening; the operational procedures associated to customer exits; the production of standardised Management Information and Reporting and some of the activities specified above, including Quality Assurance, Change and Remediation or Data Analytics.

Integrated approach to financial crime risk

Some of the most complex recent Financial Crime incidents involve a combination of stealing of credentials and impersonation, illicit use of privileged access to commit a Fraud, and multiple mechanism to launder the profits.

In that sense, a common trend in some of the most advanced financial institutions, according to regulatory advice[1], consists of achieving a convergence towards a unified Governance model that incorporates all sub-risk types (ML, TF, tax evasion, fraud and Cybercrime) into a single framework.

The natural synergies that arise by addressing the different sub-risk types of Financial Crime under a unified model and the consequent opportunity for efficiency explain the adoption of this model:

- There is a strong analysis of a new customer at the point of origination of the relationship, with a significant amount of common information cutting across customer identification, validation, name screening, customer risk assessments, etc.
- There is a component of ongoing monitoring, also with overlapping datasets around transactional and payment information, which can be merged into a single data repository for the purpose of exploitation.
- Finally, there is an investigation process that requires workflow tooling capabilities, strong record keeping, documentation and reporting.

In large financial institutions there is some level of integration. However, there is still room for improvement in terms of achieving full integration. Some of the best practices in the industry include:

- A single framework for risk identification, management and control, including a common risk taxonomy across all risk types, a common Risk and Control self-assessment, etc.
- Common underlying data infrastructure, aiming for a single, "360-view" of the customer and its data-self, together with its transactionality.
- Common framework and technological infrastructure for alert implementation and detection, as well as for alert management.
- Centralised organisations, which incentivise information sharing and a holistic approach to risk ownership and management, without gaps that financial criminals can exploit.
- Operational centres of excellence capable of providing operational capabilities across the different risk types, with cross-trained individuals capable of managing those cases.

Given the significant number of operational people currently in charge of the identification and management of the different financial crime teams, and the natural silo-ed approach with which they were originally setup, the opportunities of this journey towards integration in terms of removal of duplication, increased efficiency and effectiveness is quite significant.

[1]See, e.g. See FCA's A firm's guide to countering financial crime risks, https://www.handbook.fca.org.uk/handbook/FCG.pdf

Workforce planning and skillsets

The most advanced financial institutions have been able to connect their target ambition around AML/CTF, as reflected in their Risk Appetite and strategy, with their workforce's needs. In those cases, there is a thorough analysis that:

i. Starts with the business-wide Risk Assessment, expected business growth and changes in the risk profile and strategic initiatives that are expected to change the ways of working.

ii. Make an informed projection of the required capacity to tackle the AML/CTF strategy[61]. Some of the best practices in the industry involve the building of dimensioning models for the operational teams to be able to connect, at an operational level, demand of capacity with supply.

iii. Develops a strategy to ensure that such capacity will be in place is then designed and implemented. This includes training or recycling existing staff and hiring new talent.

In the last few years, workforce planning exercises in some of the more advanced organizations have identified the need to reinforce the teams with:

1. Quantitative and analytical profiles capable of understanding the business and the underlying risks, and building mathematical models using machine learning techniques.

2. Knowledge on specialised new payment technologies, including crypto currencies.

3. Multi-skilled individuals able of capitalize previous experience on different sub-risk types within Financial Crime, which become AML/CTF subject matter experts.

Business Processes

Financial institutions have devoted significant time and effort to streamline the business processes associated to AML/CTF. The pressure to reduce cost and improve efficiency has opened the door to advance automation technologies, business process management platforms and advanced modelling. Moreover, those improvements also have a positive impact on customer experience, 'asking things once', etc. Processes such as KYC have been significantly simplified and strengthened.

KYC: Risk Assessment, Customer Due Diligence and Enhanced Due Diligence

Delivery channels have pivoted from a branch-centered model to a self-service, non-face-to-face one, fostered by enabling technologies, institutions pursue of cost reductions, and the Covid-19 pandemic. Digital Customer Risk Management shifts from being a penalizing channel factor to become the usual means of management, which requires a stricter control over bank-customer communication. Unfortunately, it is harder for financial institutions to verify who they are doing business with and the real purposes of the business relationships. Disruptive new technologies and modern procedures allow financial institutions to mitigate their AML/CTF exposure through improved Due Diligence mechanisms. Nonetheless, some of these improvements have also become strenuous for the customer because of constant requests for documentation, often via paper with no digital alternative.

Automated self-servicing solutions[62] through digital channels, actionable by the user, using a Digital ID and Biometric data empowers customers during the onboarding process, periodic reviews and recertification. Moreover, it eases automated record keeping of customer support during due diligence process, which can be determinant in a potential investigation process. Likewise, Digital ID and Biometric data will counteract identity fraud.

These self-servicing solutions recognize the distribution of customers by segments, defined and calculated by Compliance departments backed by AI techniques. As a result, customer segmentation can improve KYC information capture aided by dynamic onboarding questionnaires. Consequently, it is key to refine the customer journey development-lifecycle, to ensure quick time to market of new enhancements in the KYC process and adapt lithely to new regulations.

KYC policies and procedures should be periodically reviewed to mitigate risk and increase financial inclusion. In this respect, some citizens are not able to open bank accounts or access to public aid because of the difficulty of gathering the required identification. Hence, financial institutions should avoid rigid, box ticking CDD measures and bet for behavioral and contextual assessments.

Ongoing Monitoring (Transaction Monitoring, Sanction Screening, Payment Screening,)

Transaction Monitoring is a heavy lifting process[63]. Aggregating all transactions, accounts, and customers in order to calculate the likelihood of each scenario requires high amounts of compute and memory capacity. Cost-benefit analysis is a contentious topic amongst Regulatory Compliance Department. Legacy systems might be enhanced to cope with performance demands, but there is a soaring necessity for cutting-edge technologies with higher provisioned capacity as more data is integrated in the models.

[61] This capacity is articulated in terms of number of people, skillsets and expertise, locations, etc.
[62] See EBA Guidance on the use of remote customer onboarding solutions. https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism/guidelines-use-remote-customer-onboarding-solutions.
[63] European Banking Authority. (2021).

Elements of human resources management

Culture and behaviors

Corporate Culture refers to the beliefs and ideas that a company has and the way in which they affect how it does business and how its employees behave [Cambridge Dictionary]

Culture, ways of working and staff behaviors have been identified in several thematic reviews and enforcement actions triggered by supervisors, regulators, and national agencies as one of the root causes of gaps in the AML/CTF framework.

For this reason, financial institutions that have advanced AML/CTF programs tend to incorporate an ambitious culture, aimed at embedding the right behaviors in the conduct of business. Some of the components of the cultural framework of the organization include capabilities around the following elements:

Staff recruitment and vetting

Before their onboarding, the individuals that will bear any responsibility associated to AML/CTF (both internal workforce or a third party) should go through a process of vetting, to validate to the extent possible that they have the right work ethic and integrity, and that nothing in their background would expose them as targets of organized crime[1].

Training and certification

Training and awareness programs involve generic courses for all the bank's employees, specific training for the AML/CTF function and training for members of the Executive Committee and Board, covering all the range of crimes and criminal strategies that are pertinent to the organization[2].

Engagement from the management

Senior management play a key role in terms of culture embedding. In advanced financial institutions, individuals that are close to the operational levels of risk framework execution feel safe escalating issues and concerns associated to business activity, and these escalations are treated anonymously and diligently. Whistleblowing mechanisms are in place and are regularly used by employees to raise concerns, or debates in decision making forums.

At a Board level, in advanced financial institutions, the Board members have both the knowledge and the management information to understand the AML/CTF risks and perform effective challenge to the executive roles.

Incentives and performance measurement

The incentive and remuneration mechanisms should be aligned to the desirable behaviors of the workforce, and to an adequate delivery of individual accountabilities as per the firm's governance model. Additionally, the incentive scheme shall not encourage unacceptable risk taking that is above the appetite of the organization.

The most advanced financial institutions have an objective setting mechanism that incorporates key risk and performance indicators associated to AML/CTF that are quantifiable, as well as qualitative indicators that reflect the desired behaviors.

Communications

As one of the mechanisms to propagate culture and to increase awareness across staff, some financial institutions build strong communication programs around their AML/CTF framework. These are run as professional communication campaigns, with a clear segmentation of the audience, selection of content to be targeted to each audience segment, delivery channel, etc.

[1]The more advanced institutions have a bespoke vetting process for the different roles within the organization, including different levels of seniority and responsibility, as well as different risks that they will be more exposed to depending on their role (e.g. customer facing clients, financial investigation unit, second line of defense specialist, etc.).

[2]The training programs might include a process for continuous review and enhancement. Moreover, there is specific responsibilities to formally review the training materials to incorporate new evolutions of the internal policy and regulatory landscape, emerging risks, new regulatory publications, etc. There are also programs for industry certifications, which can be connected to career paths and career development incentives.

A configuration to increase performance without infrastructure investment is the execution of scenarios based on customer segmentation, instead of running all scenarios for all the data available. This is harmonized with a Risk Based Assessment, because scenarios are customized to adapt to the Institution's risk profile and business reality (customers, geography, product catalogue, etc.). Another option to increase efficiency without additional resource allocation is performance simulation (number of alerts, False Positives, False Negatives, etc.) in a sandbox environment before deploying the scenario into Production. A third option is to run the scenarios only against susceptible customers, omitting, for instance, government and public agencies with very low risk. On a related note, potential links with sanctioned entities could be identified through retroactive batch screening over the complete customer portfolio, considering those customers as high-risk individuals to be investigated.

The business processes around sanctions have suffered a significant transformation in the last months, as a result of the Russia invasion of Ukraine, and the associated legislative actions that the European Union, the US, the UK[64] and other geographies took. Financial institutions have invested resources in both interpreting the restrictions and in operational improvements in terms of list management. In some cases, this has meant an acceleration of programs aimed at implementing a Centralized List Management Platform that aggregates files from different treasury departments and vendors, cleanses the data and then disseminates them amongst all group entities according to their local regulations and the group's policy eliminates duplicities and increases oversight of the Sanctions program[65].

Transactional scanning[66] and customer name scanning during onboarding shall run in real time. Therefore, strict Service-Level Agreements (SLAs) are required for list upload, as most systems cannot scan during a list refresh. On the other hand, when black or grey lists are updated, a batch scanning is required on all customer records against changes in the lists. This process should not interfere with the online processes and should run on a separate queue, as lists changes are very frequent, even several times a week and time consuming, given the high number of customer records.

Alert Management and Investigation

The implementation of a specialized vendor solution per module, and at times more than one tool per module from different vendors, isolates alerts as Case Management systems are not integrated. What is more, Compliance Officers do not have access to all the data and their procedures may vary due to their tool. To gain a holistic view of the customer risk and standardize alert investigation and reporting, it is indispensable to consolidate KYC, Screening, Transaction Monitoring, and Alert & Case Management data into a single platform. Consolidating basic information required for an investigation before the alert is assigned enhances the time per alert plus automatic notifications to the compliance function when an alert is pending authorization.

Machine learning models are helpful to score alerts, in order to discriminate potential false positives. Then, the Compliance department should have established a clearly defined and objective workflow for the review of alerts, with a prioritization criterion to analyze them[67].

Engagement with Law enforcement and Suspicious Activity Reporting

Even if risk detection is successfully implemented, bad reporting could tamper the process. Financial institutions must comply with their FIU's expected SLAs, adapting their reports to a specific format that is subject to changes. Some regulatory steps that do not require manual intervention, for instance Currency Transaction Reports (CTRs), applicable in USA, leave room for automation. At the same time, proactive detection of CTR Exemptions is a quick-win enhancement of the CTR function. Nonetheless, AML Management should periodically review the decision-making process of exceptions to gain control and understanding.

[64] See the Economic Crime (Transparency and Enforcement) 2022 Act (the ECTE Act) in the UK, OFAC Frequently Asked Questions 1007 and 1010, or the up to eight packages of sanctions imposed by the EU on Russian individuals and companies.

[65] Sanctions platforms need customization rules to avoid scanning irrelevant values (PO Box, #, double spaces…).

[66] In addition to the analysis of money transfer, the digital footprint is a rising method for red flags. The IP Addresses collected during customer's operations, associated with transactions and logins, shall be routinely monitored and compared with the ones ingested during onboarding to detect misuse of an account from a High-risk/Sanctioned country or account theft. The detection of Tor associated IP addresses is fundamental, as it might reveal connections between the customer and criminals from the darknet.

[67] For example, based on risk profiles, transaction amount or matching scores). This process is only possible if carried by specialized AML teams to handle the sleuth of complex organizations and manage whitelists.

Communication with the lines of business, who have a direct contact with the customers, demands dynamic channels to resolve questions and transfer documentation within the regulator's timeframe, and applying penalizations on client managers in case of frequently repeated mistakes when collecting customer information. Finally, repeated warnings and foundations of rejected reports require detection and data profiling to understand the root-cause and palliation. Data Quality between ATMs and Bank databases with previously recorded customer information is important, but also to identify reporting mistakes and duplicities before filing them to the regulator.

Management Information and Data

Management Information

The Management Information on AML/CTF enables measurement, visualization, communication and effective management of the underlying risks. In that sense, the best practice in the industry includes the adoption of industry standards around data governance and management and reporting practices (e.g., BCBS 239[68]).

The management information produced should detail the changes in the Risk Assessment at a firm-wide level, as well as a representation of the risks associated to new business relationships (including new business relationships per risk category, any new high-risk relationship, etc.). For existing relationships, the top management of the organization should receive timely information on the outcomes of the ongoing monitoring activities (e.g., transaction monitoring, payment screening, periodic customer reviews), as well as the summary of the Suspicious Activity Reporting (SAR) and statistics on positive hits above and below a specific threshold. The reporting structure should also contain the exit of existing relationships, and its rationale.

In particular, the more advanced financial institutions incorporate, in the reporting to the Board, Board delegated Committees and Executive Committees, a comprehensive set of metrics and qualitative information to ensure that all the underlying risks associated to the business are taken into consideration. Additionally, for more operational teams, institutions have developed dashboards containing real time KPI and KRI metrics, with the option of extracting insights on the data in more detail to facilitate the identification of weaknesses in the process and draft long-term strategies.

Other good industry practices include the incorporation, in the regular management information escalated to senior management, of the open issues at portfolio level stated by Quality Assurance, Internal Audit or Supervisory investigative action[69]. This view also overlays, on top of the remedial action, the information on strategic transformation of the AML/CTF operations and provides in this way a single view of change across the discipline.

[68] Basel Committee (2013a). https://www.bis.org/publ/bcbs239.pdf

[69] In the more advanced organizations, the reports to senior management include a section on Regulatory Liaison or Industry engagement. This usually contains an element of horizon scanning for new regulation or legal requirements (and the anticipated downstream impact in the organization).

Data Management and Data Quality

Data has been one of the key areas of evolution and investment by financial institutions in the last years. There is recognition that insufficient or poor-quality data[70] is one of the most relevant factors that impact the ability of a Financial Institution to identify, manage and control ML/TF risks. In addition to classical, manually driven data quality remediation, firms are making extensive use of advanced techniques for data discovery as well as analytical methods like fuzzy logic or natural language processing to perform data matching and harmonization.

There are several Data Management capabilities supporting the AML/CTF functions that are instrumental. One of them is a Data Quality capability to proactively specify business rules and data quality standards around the critical data elements used in risk identification and management. Also, a Data Catalog that allows harmonization of data across different repositories and engines and allow data stewards to better understand the business meaning of the data, classify the data collected and consumed in each process, and alert appropriate stakeholders in case of a data issue. Moreover, financial institutions are investing heavily in data lineage capabilities to enable end-to-end traceability of the data from the point of use back to the point of origination.

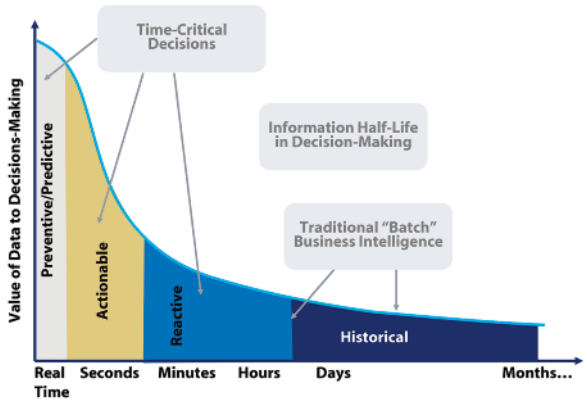
Even the most advanced AML/CTF systems' automatic detection are not trustworthy if the data is wrong. Quality rules implemented on the transactional, front office systems will ensure the correct data generation and consistency rules will confirm the right data feeds into the AML/CTF systems.

Data infrastructure and demands on an AML/CTF Data Model

The need for Management Information implies a demanding data infrastructure[71]. It is desirable to capture, store, process and manage sensitive information with the highest standards. The technological modules used for AML/CTF can excel at their analytical capabilities, but duplicated data flows to different, siloed technological component is highly inefficient from the transmission standpoint.

For this reason, it is important to have a unique data repository accessed by all technological components and business processes involved in the AML/CTF framework. This way, each process (e.g., Customer Risk Rating, Alerts, Case Results, SAR, etc.) uses data from the central repository and store their results back in the same repository, making them instantly available for other processes and parties involved. Financial institutions that operate in multiple countries can centralize their tools and repositories for whole regions or even globally. These solutions will improve compliance oversight, and reduce costs in duplicated vendor licenses, infrastructure or departments in the group entities. Therefore, leveraging these external sources to complement the available internal information is a trend in most financial institutions.

Figure 3. Time reduction of value of data for decision making.



Source: Perishable insights, Mike Gualtieri, Forrester

However, financial institutions can no longer obtain by themselves all the necessary information to properly identify and assess potential risks inherent to their activity. In a digital-centered industry, accumulated data can be sold or shared with other parties. Hence, external sources such as reputed bureaus, national crime agencies, court judgments and public registries are recommended sources for model enrichment.

Disruptive technologies, modern customers' behavior and natural disasters require financial institutions to redesign their transaction monitoring strategies. Models undertrained on new AML/CTF techniques do not provide the ability to respond rapidly to Financial Crime risk. Consequently, certain scenarios should automatically execute when particular external events occur (new products, lockdowns, catastrophes, conflicts etc.).

Historical analysis is a key practice in these cases. Even if the financial institution misses any scenarios during a crisis, red flags can still be found against these temporary scenarios and SAR submitted. Behavioral Monitoring is one of the current trends in the industry, supported by the newest machine learning techniques. Behavioral Monitoring first defines how the products and services are expected to be used. Secondly, it looks at historical behavior, expected behavior, peer-group behavior and identifies behavior changes, consuming all available data to detect Financial Crime risk.

In the Case Management area, the widespread use of social media is again requiring for the ingestion of unstructured data and the use of graphs to find potential connections between customers and criminals. Finally, standardized reporting templates using data pooling tools, which combine datasets from multiple sources, and automated generation of SARs will accommodate any format changes required by the FIUs, reducing rejections.

[70] Basel Committee on Banking Supervision. (2013b).
[71] Basel Committee on Banking Supervision. (2013c).

Technological infrastructure

AML/CTF tools can no longer rely only on a relational DataMart as a central database, as it is now receiving unstructured data where NoSQL and Data Lakes become more effective. It is of utmost importance to implement real time detection technologies to prevent risks associated with unnoticed errors and improve customer experience (see figure 3). Financial institutions still rely on queuing and file management systems to send transactions and notifications between applications. Transactional and name screening (or cases outside AML/CTF, like Fraud audio detection) benefit from real time analysis. For the latter, machine learning libraries for Natural Language Processing (NLP) are appropriate to collect, analyze and store audio information and, create alerts to the lines of business interacting with the customer, finalizing the call immediately to avoid sharing any personal information (figure 3).

Real time and unstructured data improvements result on spikes in transmission, processing, and storage activity, with major investments in new storage options and data migration. For this reason, migrating to a Cloud infrastructure is a sound solution to access new features for data management.

Regarding IP address screening, financial institutions need to coordinate amongst them and regulators to systematize the generation of lists containing non-trusted IP addresses, IP addresses from sanctioned jurisdictions or IP addresses flagged as suspicious. Alongside, analytical tools are available in the market to detect if customers are using a Virtual Private Network (VPN) to distort their real location. Application-programming interfaces (APIs) play a significant role in this new monitoring, as their logs should capture IP data that can be analyzed in real time, employing tools such as AWS OpenSearch or Splunk.

Robotic Process Automation (RPA) is one of the main technological trends that increases customer experience through automated self-servicing solutions. Virtual agents, chat-bots and call-bots can assist customers with structured and repetitive inquiries day and night without interruption, getting them in contact with a human resource for queries that are more complex. RPA is also a crucial improvement for Alert and Case Management, as these algorithms can ingest more data from more sources quicker than a human investigator, enabling faster analysis of a broader evidence base and, ultimately, more accurate resolution[72].

[72]For example, collecting and aggregating necessary data for an investigation, saves time to the AML Officer searching for documentation. Other repetitive tasks are subject for automation, for instance, flagging duplicated alerts of a single customer. More sophisticated systems will automate steps or results based on previous investigations and outcomes.

Some examples of data requirements and practices

Some jurisdictions such as the EU (e.g.: eIDAS) require financial institutions to capture and manage eIDs from any Member State for AML/CTF purposes, which is expected to reduce costs and human errors with better customer experience. This is significant for trust services, which are deemed to have higher risks due to their structure, short lifecycles and varied purposes.

In this respect, during any business relationship, financial institutions collect geolocation and IP Address information to later detect activity from undesirable locations or account theft. A robust Data Integration capability correctly connects the different fields with the questions shown in the dynamic questionnaires, thus segmenting the customer. FinCen[1] even recommends collecting the IMEI (International Mobile Equipment Identity) a unique 15-digit identification number assigned to each mobile phone, and device model of the customer's cellphone for convertible virtual currency operations. Financial institutions store their digital interactions with customers deploying semi-structured and unstructured databases.

As mentioned, financial institutions have to integrate information from external sources to enrich their models. Some of this information is easy to ingest, such as ultimate beneficial owner flags in public registries or records from a PEP list. Conversely, Adverse Media files can include audio or video format, which again highlights demand for unstructured information. Additionally, some jurisdictions require automated mechanisms to report any misalignments between public registries and data collected by obliged entities.

In terms of screening lists, there are also some industry good practices worth highlighting. Blacklists must not be modified, except for enrichment and aggregation, whilst white and grey lists shall be quick and easily updated by Compliance departments to improve performance and comply with internal policies. This perspective has to be reflected when building a centralized list management system jointly with automatic notifications when lists are received, aggregated and disseminated. Statistics about record counts should be available and the system should expect automatic notification from the screening systems, reporting same list record counts loaded on their databases.

Other than that, in 2018, OFAC included the first virtual currency addresses in the SDN (Specially Designated Nationals and Blocked persons) list. These are digital wallets tied to sanctioned individuals and companies with whom businesses is prohibited, which structure is as described. These are digital wallets tied to sanctioned individuals and companies with whom business is prohibited.

One of the most relevant industry trends is the adoption of ISO20022 on SWIFT payments, which improves screening and monitoring performance by including XML tags. By contrast with current free-form messages, SWIFT payments will clearly specify the meaning of the fields, reducing false positives. Financial institutions are required to upgrade their screening and monitoring systems to parse these new tags and store them in appropriate tables and columns in their databases.

Reference of new SWIFT transaction information XML tags.

Digital Currency Address	XBT	158treVZBGMBThoaympxccPdZPtqUfYfT9
SDN list column	Currency	Wallet ID

[1]The Financial Crimes Enforcement Network of US seeks to safeguard the financial system from illicit use, combat ML and its related crimes including terrorism, and promote national security.

Analytical modelling and advanced techniques for AML/CTF

"A model is always partial, but it offers resources for advancing knowledge"
Jean-Pierre Changeux[73]

This section describes some of the trends and more innovative industry practices based on analytical modelling and advanced techniques for the identification, management, control and oversight of ML/TF.

The context for the analytics approach to AML assessment

With the emergence of more restricting regulation, aiming for a quicker and better identification of risk, and new technologies available, financial institutions are moving along a new transformational journey regarding the implementation of adoption of advanced AML analytics[74]. The three primary tools used to detect ML include the customer risk rating, the Transaction Monitoring, and the Sanction Screening rules.

Customer Risk Rating

The customer risk rating is a model based on the risk drivers associated with the ML identification, such as customer's country, occupation and salary, banking products, etc.

Statistical models have become the mainstream practice for customer risk rating, by the application of different techniques to solve the anomaly detection issue. However, this problem is complex to identify or reproduce, and produces imbalanced samples.

The application of advanced data methods allows us to overcome these limitations, improves the customer risk rating accuracy and fosters its relevance along the AML program. The customer risk rating progressively evolve to a behavioral customer risk rating in which continuous data is updated and enriches the risk identification process[75]. Furthermore, models themselves are incorporating the benefit of using machine learning techniques. Supervised methods, such as random forest, are the first to be implemented to unveil hidden relationships between risk drivers in an augmented set of factors.

As the computational power, richness and depth of the data increases, these behavioral models can also incorporate triggers for potential transaction structuring, namely, collective strategies to launder money by multiple individuals through small amounts, to avoid detection by classical static detection strategies. The ability to build algorithms and strategies that run, not at an individual customer or customer plus transaction basis, but on ensembles of customers enables the identification of transaction structuring in a more proactive and effective way. These so-called graph algorithms[76, 77] leverage upon potential connections coming from different sources of information[78]. Moreover, the ability to build a comprehensive network representation of all clients brings the additional value of streamlining the process of alert investigation, amongst others.

Transaction monitoring and filtering

The most common approach to transaction monitoring and filtering consists of a rule-based system, in the style of a decision tree. Each rule is configured to identify a defined behavior masking potential ML activities of the customers and entities involved in the transaction[79]. These rules are generally identified as "scenarios". More complex rules and scenarios try to address the identification of nested accounts and more sophisticated

[73] Jean-Pierre Changeux (b.1936) is a French neuroscientist known for his research in various fields of biology, from the structure and function of proteins, to the early development of the nervous system, to cognitive functions.

[74] However, there is not uniformity in the degree of adoption of these advanced analytical techniques. While some financial entities are experimenting with innovative solutions, simple applications are more usual in the industry, and the reliance on analytic support is at its inception for others. Nevertheless, the present and future of the AML/CTF programs cannot be understood without looking at the new technologies and methodologies available.

[75] For example, incorporating information from transaction monitoring, payments screening or outlier analysis around channels, volumes, geolocation, etc.

[76] Soltani, Reza & Nguyen, Uyen & Yang, Yang & Faghani, Mohammad & Yagoub, Alaa & An, Aijun. (2016. 1-7. 10.1109/UEMCON.2016.7777919.

[77] Scalable Graph Learning for Anti-Money Laundering: A First Look; Weber, M; Chen, J.; Suzumura, T.; Pareja, A.; Ma, T.; Kanezashi, H., Kaler, T.; Leisersen C.E.; Schardl, Tao B.

[78] For example, closed circuits of transactionality – regular transfers-, to joint accounts ownership, single address, branch of choice or mostly visited branches or ATMs, geopositioning via mobile app, coincidence of merchants, etc.

[79] This suspicious behavior will be most likely based on outliers on location, transaction count or transactions amounts.

relationships between parties, but the basis of the outlier identification broadly remains at individual transaction level by looking at the data received during the transactional process. When an outlier is identified, an alert is triggered, which subsequently requires expert evaluation[80].

In this process, the initial set of rules is broken down into a deeper segmentation of behaviors in which the line of business, the level of transactional activity and the risk assessment of the customer determine the final behavioral outliers, i.e., the alerts that would be trigger.

Data analytics methods can be leveraged to detect more quality alerts, increasing true positives and reducing false negatives, i.e. more true alerts are identified without increasing the noise in the identification. Data analytics and machine learning techniques are implemented to optimize the segmentation providing more accurate identification of patterns thanks to the exploration of historical data[81].

Nevertheless, financial entities actively looking into incorporating advanced methods in their AML/CTF program might decide to focus on alert prioritization. The rule approach generates large amounts of alerts even when proper tuning of the scenario thresholds is implemented, and segmentation has been optimized. To address this, many banks implement supervised learning methods to rank alerts in terms of productivity[82]. The key aspect that determines the success of this approach is the utilization of differential metrics, beyond the expected and immovable variables available at transaction level.

The most disruptive approach to AML risk identification consists of abandoning the traditional individual rules approach to unveil hidden relationship with advanced analytics. However, few financial institutions are exploring the utilization of alternative methodologies. Some of these are:

- Graph analytics, which are taking their space in the identification of network relationships and are increasingly determinant of ML activities in the interconnected financial world.

- Clustering techniques, which help to identify outliers without assuming specific behaviors; therefore, capturing more frequently potential new illicit activities.

Advancing towards a non-rule-based approach does not automatically imply abandoning previously identified good optimization practices. In fact, reliance on advanced analytics to improve the customer segmentation, combined with network and outliers' detection, together with the utilization of alert prioritization could be seen as an integral solution.

Sanction Screening

The Sanction Screening engines compare individuals or companies against designated sanction list using fuzzy matching techniques. The most straightforward approaches are based on a wide range of transformations applied to the "names" (name order change, initials, transliteration, common vocal or consonant mistakes, etc.). The transformed names are standardized as strings and compared with the names in the sanction list, also standardized following the same rules. The

[80] See Scalable Graph Learning for Anti-Money Laundering: A First Look; Weber, Chen, Suzumura, Pareja, Ma, Kanezashi, Kaler, Leisersen Schardl, Tao.

[81] Data driven threshold tuning allows to optimize the buckets of increasing productivity along the variables used in the scenarios (more true positives) while providing measures of the potential risk not identified (limiting the false negatives). These common approaches rely on the existing rule-based engines.

[82] This approach may be seen as an imitation of the level 1 analyst review of alerts; however, this could be a more complex identification to address and not all the entities succeed in this effort.

An example of National Risk Assessment

The UK government regularly publishes a national risk assessment[1], which informs on the risks faced at a national level in Financial Crime. This national risk assessment provides references on the most common ML/TF techniques used and their level of implementation in the country and is an important reference for the institutions themselves in their risk assessment.

A firm must perform a Financial Crime risk assessment and use this to inform the design of their AML controls. The national risk assessment therefore serves as a strong foundation to build this assessment from, with the firm taking extra steps to understand, more specifically, the risks they face.

This would take into account, but not limited to, their portfolio of clients and the products they have - personal current accounts serve as a means of tax evasion for many small businesses as well as introducing exposure to many other money laundering techniques due to their ability for rapid fund transfers and accepting cash transactions. Additionally, a review of historical criminal activity can help understand any additional typologies faced by the bank.

Cash transactions, in and out of accounts, serves as an easy way for money launderers to break transaction trails. Whilst the use of cash in money laundering is widespread and is included in many of the strategies used, the controls around cash risks are usually the simplest largely due to the little information available for cash transactions.

Money mules are third parties that are either wittingly or unwittingly used to make additional cash transactions and fund transfers that mask transaction trails. This can be used in conjunction with other strategies, e.g. purchasing high value, resalable assets, to almost completely remove suspicions of the source of funds, where the temporary accounts could be those of a mule network. This is difficult to detect using traditional methods as no single account, and no single customer, may ever be used for large volumes of the transactions used in any stage of this process.

Similarly, cash-intensive businesses serve as another challenge for traditional detection methods. Businesses such as beauty salons, newsagents and car washes are used by money launders to document cash made from criminal activities as legitimate business proceeds so that large volumes of the criminal network's illicit funds can be centralized into one account. This proves difficult to detect as the business's cash income may seem consistent with its own history as well as the income of its peers, and therefore there may be no suspicions raised by the cash transactions of the business. These businesses, however, are commonly also linked to human trafficking and modern slavery, which include their own transactional behaviors that may be easier to detect. As with the usage of money mules, these typologies will commonly involve a network of seemingly unrelated third parties. These third parties may be the facilitators or even the victims of these crimes and therefore there are specific behaviors one would expect to see. Transactions in multiple different cities, especially in cities with transport hubs, heavy usage of fast-food restaurants, multiple transactions in the same hotel on the same day, multiple payments to mobile providers, fund transfers between accounts with similar behaviors, and international transactions especially cash and fund transfers are all strong indicators of these typologies. If these parties can be linked to the cash-intensive business, then the full network could be uncovered.

International transactions are another high-risk transaction identified in the national risk assessment. These are seen in a variety of machine Learning techniques, as well as presenting a risk in other aspects of Financial Crime. This is seen in human trafficking, which is estimated to be one of the largest generators of criminal proceeds globally. Human trafficking requires sending money abroad to members of the associated organized crime gang in the countries associated with the trafficking. This may be as cash withdrawn in the UK and physically moved abroad or via money mules in a similar way as the behavior associated with cash deposits previously described.

Terrorist financing is identified as a high-risk typology within the UK. The raising and moving of funds are not considered a primary goal of terrorists, especially since the majority of recent terrorist attacks have been low-budget and low-sophistication, frequently planned, funded and done by an individual. Terrorist financing is commonly used for moving funds abroad through relatively simple methods such as physically moving cash abroad or employing MSBs. Therefore, detecting terrorist financing requires a collection of key indicators in the same way as required for the usage of cash-intensive businesses in money laundering.

The risk associated with crypto assets grows year-over-year as crypto assets become and more common and easily accessed, but the controls around them remain relatively new with the UK introducing regulations around the usage of crypto assets for money laundering only in January of 2020. Organized criminal gangs use crypto assets for money laundering by first purchasing the crypto assets with their illicit funds, potentially after an initial stage of layering, before selling the assets to provide a legal source of their funds. Additionally, crypto assets can easily be moved across borders allowing criminals to move significant funds internationally with significant ease in comparison to fiat currencies.

This serves as an example of new emerging risks in Financial Crime presenting another challenge for firms to develop and action new controls on a regular basis to keep up with the changes and developments found by money launderers.

[1]HM Treasury: National risk assessment of money laundering and terrorist financing 2020. December 2020.

matching rules or logics measure the degree of separation between the two strings. The engine may return a score of the matching, or an alert based on a pre-defined rule of matching, however, the underlying rationale is the same, i.e., the two strings are similar enough to grant an expert review.

As in the case of Transaction Monitoring, these rules produce a large number of false positives[83]. Furthermore, the potential for optimization based on tuning is lower than in the case of Transaction Monitoring.

For this reason, entities are exploring alternative methods to improve the quality of identification based on translation and transliteration technologies, and the application of NLP techniques to improve the name matching. The improvement in the analytical methods for Sanction Screening run in parallel with the exploration of these techniques in the identification of negative news.

The next steps into analytical approaches to AML/CTF assessment

The application of innovative methods and technologies does not stop at the ones highlighted above. Extended natural language processing and deep learning, blockchain applications, electronic verification of identity, voice and speech recognition, biometrics, or geolocation are other technologies that may contribute to the identification of illicit activities.

Underlying to all these potential approaches, several trends in AML/CTF analytics can be found:

- Deeper analysis of existing data both at the transaction moment, and from the moment the customer and their relationships are implemented. Some of the analytical options outlined above become powerless if differential data is not available and incorporated into the analysis.
- Supplementary data from the internal sources and the different dimensions of the AML/CTF program (i.e., customer risk rating, due diligence, sanction identification, transactions) and external sources (public data on PEP, ownership relationships, reputational sources, open searches) is required to create a holistic approach to the AML/CTF risk identification.
- Technologies and methods can be as complex as innovation allows, however dimensioning the most adequate ones to the nature of the business and risk assessment of the institution is critical to optimize the use of technological and human resources while ensuring regulatory compliance.

[83] Engines can be more or less complex in the incorporation of innovative transformations applied to names, or incorporate more quality sanction sources improved with PEP information, however, they all exhibit the same weaknesses.

Supervisors and regulators are in general reluctant to sudden changes and favor well-stablished methodologies before fully embracing revolutionary changes. However, for those institutions willing to embark in a full transformation program of AML analytics, a number of advances have taken place in recent years[84]: from specific developments of fuzzy matching applications or PEP screening in joint collaborations, to the constitution of innovation centers and sandboxes.

In the journey towards more sophisticated risk identification, interpretability and appropriate risk control remain at the core of the regulator's concerns (and of the institutions).

The use of advanced analytics in the AML/CTF program is linked to the consideration of the implemented rules as models and are therefore subject to the identification, monitoring and control practices that entities have deployed under the Model Risk Management (MRM) function. While the distinction for the customer risk rating is clear, as it fulfills all the conditions typically established in the model risk management (MRM) framework to be a model or at least a user tool that should be monitored, AML/CTF engines have not been initially seen as models. The assimilation of the AML rule engines in the model risk management discipline has not uniformly happened across jurisdictions and main players want to avoid the burden on an incremental scrutiny of the AML programs[85].

Nevertheless, the machine learning technologies to improve risk identification are broadening the conception of what is meant by a model subject to MRM. Despite their willingness to foster their application to AML/CTF programs, supervisors make clear the need for ensuring a proper degree of understanding and interpretability of the methodologies implemented and outputs obtained. Black box models are to be avoided. Machine learning models may suffer from a lack of transparency in the feature selection and explainability, model performance evaluation, etc. Appropriate documentation, testing of the model, interpretability modules; the basic principles of a robust MRM framework will support the adequacy of these models for the AML/CTF use.

Use Case: Enhancing suspicious pattern detection through network analysis

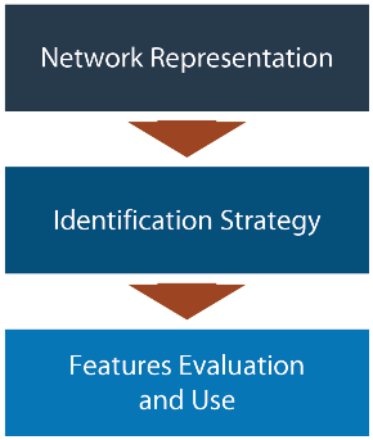
As explained before, one of the primary tools to detect ML is transaction screening and filtering. Whithin this tool, the commonly approach to identifying suspicious ML behavior by fixed patterns of transactional movements, previously described, is being progressively enriched by combining more powerful analytics. The utilization of network analysis for example has been proven to help in the characterization of ML patterns with unique metrics or features. The enriched features may be used in rule-based approaches or in more complex techniques such as machine learning or fuzzy algorithms.

Three relevant stages are at the core of the integration of network analysis in the ML detection: (i) collection of relevant data and construction of the graph representing the relationships between the entities involved; (ii) definition of the identification strategy that would allow to identify the cluster of entities and relationships which are suspicious; and (iii) characterization of those clusters by appropriate metrics which will be used as features of the ML detection models (see figure 4).

Stage 1: Network representation

A network allows to examine complex relationships between related entities, either through links of internal data, such as transactions, or external data, such as addresses and ownerships

Figure 4. Stages for detection by network analysis.



[84] In words of the recent paper issued by FATF, "new technologies have the potential to make AML and counter terrorist financing measures (CTF) faster, cheaper and more effective". Additionally, the FATF enumerates the multiples initiatives of worldwide supervisors and entities that constitute the forefront of the industry evolution See: Opportunities and challenges of new technologies for AML/CTF, available in https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CTF.pdf .

[85] A join statement by the FRS, FDIC and OCC addressed industry questions on how the MRM guidance should be applied to BSA/AML compliance models. The supervisors consider that not all the systems are required to be classified as models, and the bank itself may categorize models as they see fit. Most importantly, they stated that the banks are not required to have duplicative process or conduct duplicative testing activities to comply with BSA regulations. Although providing certain degree of maneuvering to financial institutions, the statement reinforces the view of bank addressing the risks associated to the AML systems (models or not).

(see figure 5). The construction of a network requires to compute sufficient granular data points that could connect the entities with different objects such as companies, addresses, digital uses, etc. and consider the strength of these relations (e.g., transactional connection). This network can be structured as a graph (both directed or undirected, and weighted or unweighted). The network constructed and the information contained within it will determine the suitability of certain techniques (for example, a weighted undirected graph could be treated in the following steps using clustering techniques, such as spectral clustering).

Stage 2: Identification strategy

An identification strategy is needed to uncover potential money laundering or other illicit activities' patterns within the identified network. There are different strategies that can be used, for example:

- Heuristic approaches based on proximity to confirmed suspicious cases or entities
- Probabilistic approaches and pattern recognition
- Community detection approach, leveraging on machine learning techniques

When implementing the community detection approach, the different communities need to be discovered. A community is a subgraph in the network with a higher number and more intensive relationships among the members of the community compared to random, uninformative subgraphs (see figure 6). Community detection is a useful approach to detect and characterize the targeted structures, which may require the use of algorithms such as k-means, hierarchical clustering, spectral clustering, evolutionary algorithms, or modularity optimization[86].

To find optimal communities, a specific function is optimized: the Modularity Formula. Given a network represented as a weighted graph and partitioned into communities or modules, this formula depends on the specific structure of the graph representation, and expresses the mathematical definition of modularity in terms of weights:

$$Q = \frac{1}{2w}\sum_i \sum_j \left(w_{ij} - \frac{w_i w_j}{2w}\right)\delta(C_i, C_j)$$

Where Ci is the community to which node i is assigned, w_ij represents the value of the weight in the link between the nodes i and j (0 if no link exists), $w_i = \sum_j w_{ij}$, and $w = \sum_i w_i$. Finally, the function δ corresponds to the kronecker delta function: $\delta(i,j)$ takes the value 1 if the nodes i and j are in the same module and 0 otherwise.

Stage 3: Use of features

Once the target communities have been identified within the network, specific metrics or features can be defined to evaluate the depth and importance of the relationships, or the risk of the connections between entities. These features can be used in rules or machine learning algorithms to enhance the predictive capabilities of the models by reducing false positives and identifying better suspicious patterns. The rule-based approach incorporating "enriched" features may be useful to produce qualitative alerts as they incorporate new information apart from the traditional transactional base related to the customer (see figure 8). However, machine learning techniques can unveil stronger relationships which allow to separate true positive alerts and false positive alerts.

[86]Optimal algorithm for pattern detection have been developed by several authors. See L. Alsedà, A. Awasthi, Jörg Lässig (2012).

Figure 5. Depiction of community detection algorithm (steps (a) to (d)) using the modularity optimization.

The upper community contains a suspicious behavior (target) corresponding in this use case to the Customer A network of Stage 1 (shown in figure 7 in the next page).

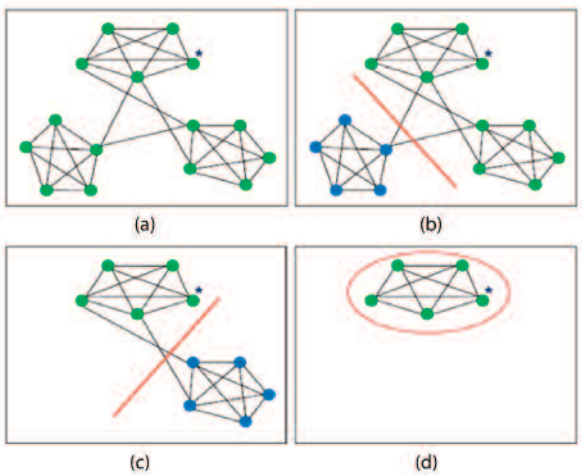
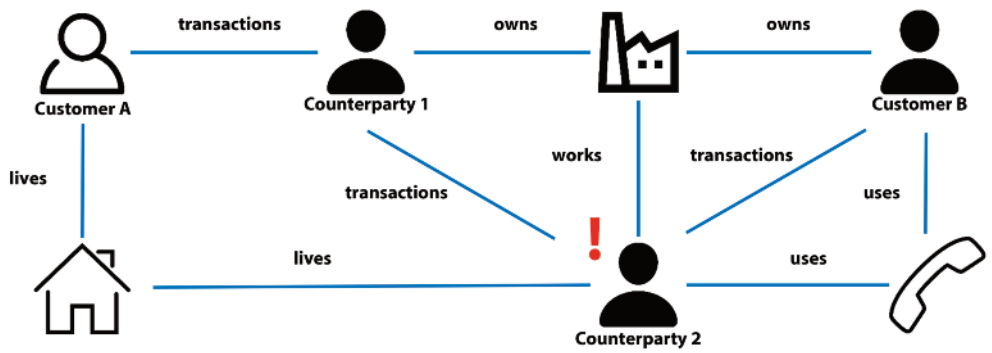


Figure 6. Simplified logic for a scenario based on features obtained through network analysis. Other features such as transactional amounts, may be incorporated according to the pattern or combination of patterns to be detected. This example is for illustration purposes only.

Logic and Parameterization of detection rules with network features:

- If entity type = **Individual**
- If suspicious community identified: suspicious connections identified = **Yes**
- If number of paths to suspicious node > = **num_paths_to_suspnode**
- If distance to suspicious node is <= **max_dist_to_suspnode**
- If primary connections to suspicious node = **primary_connection_type**

Figure 7. Depiction of network relationships related to Customer A including a suspicious node (Counterparty 2 is blacklisted) and possible synthetic entities (nodes related to the Company).



In the example shown opening this user case, figure 7, whose network information is presented in figure 8, Customer A and Customer B pertain to the same suspicious cluster with connections to the suspicious entity (Counterparty 2), but Customer B has the strongest relationship, both personally and professionally with Counterparty 2.

Based on this scenario, if thresholds were calibrated to be num_path_to_suspnode = 1, max_dist_to_suspnode = 5 and primary connection to suspicious node = "all" (either transactional, personal or any type), then both Customer A and B will be flagged as suspicious entities (or their related transactions, etc.). However, considering a more traditional approach, without using the network analysis, only Customer B would be flagged; Customer A does not have transactional connections with the Counterparty 2.

Complex features can be evaluated and different types of machine learning algorithms can be trained resulting in higher risk assigned to Customer B and associated transactions. Incorporating new features into the models also allows to increase the accuracy and detect more potentially risky behaviors (reducing false negative alerts), while discriminating better the risk among those behaviors identified (reducing false positive alerts).

Figure 8. Information on customers for suspicious connections identification.

Entity	Min distance to suspicious node	Primary connection to suspicious node	Personal data connection	Number of paths to suspicious node	Cluster identified	Suspicious connections identified
Customer A	2	Transactional	Yes	2	1	Yes
Customer B	1	Transactional	Yes	4	1	Yes

Conclusions

Financial Crime (in its broad sense, including money laundering, terrorist financing, breach of economic sanctions, bribery and corruption, fraud and market abuse) continues to be a major threat for the financial sector across world, and in particular money laundering as one of the areas to pay more attention to. According to the United Nations Office on Drugs and Crime, the amount of money laundered globally in a year is estimated to reach between 2% and 5% of global GDP, or between $800 billion and $2 trillion in current US dollars. With less than 1% of it ever seized or frozen by law enforcement agencies.

Financial Institutions, regulators and crime agencies are working together to leverage upon stronger computational capacity, more advanced mathematical modelling, increased awareness at senior level and stronger coordination to fight Money Laundering across jurisdictions to combat this economic crime.

In this context, financial institutions are investing in improving their capabilities to be able to identify, manage, measure, control and monitor their risks:

1. Framework and Governance, with more formal and comprehensive risk assessments, more granular standards and policies, a better defined and more coordinated three lines of defence model and, more integrated approaches for Risk Management (across different economic crime risks).

2. Organizational structure, with specialized, fully devoted teams led by subject matter experts in the field. Also the centralization of capabilities to ensure efficient and effective action, and the strategic workforce planning that ensures not only the current supply of subject matter experts, but the identification of future needs of skills (e.g. data scientists). Financial institutions are also investing heavily in ensuring adequate internalisation of the right culture and behaviors to tackle this crime.

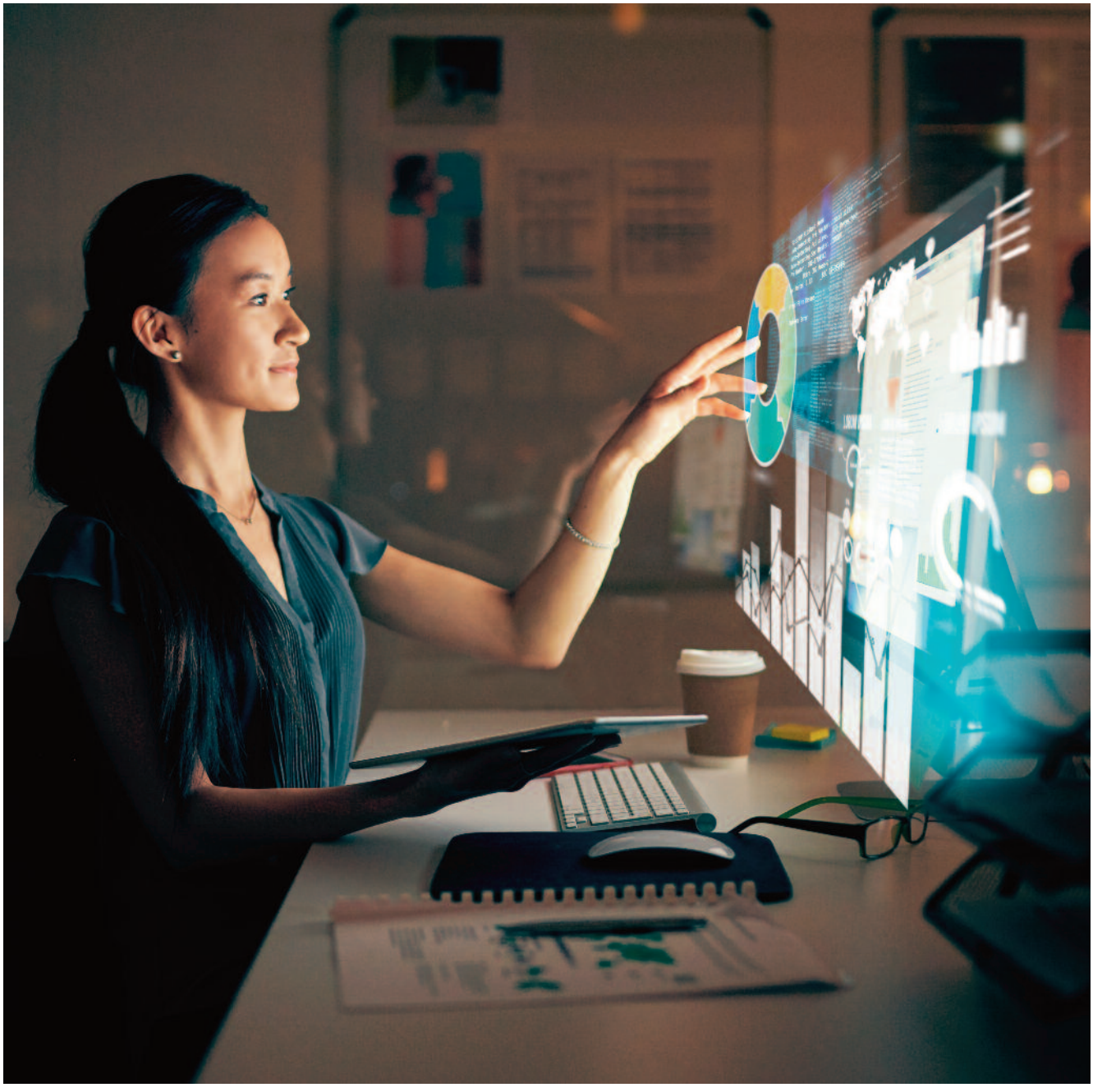
3. Business processes, including firm-wide risk assessments as well as individual customer due diligence and risk assessment. Also the investment in streamlining and strengthening the Transaction Monitoring, sanction and payment screening, alert management investigation as well as the engagement with law enforcement.

4. Improvement of the underlying data fabric that supports risk identification and measurement, including improved data sources, better data quality and data governance capabilities.

5. Investment in the technological infrastructure, with specific focus on being able to cope with new threats such as money laundering through cryptocurrencies, in addition to increasing capabilities and automating the technological processes.

One of the main areas of investment, which is also proving to be one of the most effective, is the development of advanced analytics modelling to increase the effectiveness of the detection of threats. That is one of the pillars of the future of an effective money laundering (and broader financial crime) function: one where data, advanced analytics and modelling are able to identify patterns close to real time and trigger productive alerts and automated responses.

Glossary



AML: Stands for Anti Money Laundering, it is mainly used in the financial, legal and compliance sector to refer to the standard controls that companies and organizations must have in place to prevent, identify and report suspicious money laundering or money laundering behavior.

BPM: Business Process Management. BPM is a working methodology based on a management system that is responsible for controlling the modelling, visibility and management of the company's production processes.

BSA (Bank Secrecy Act): From 1970, it is one of the first laws to fight money laundering in the United States. The BSA requires businesses to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory matters.

Convention on Transnational Organized Crime: It was adopted by General Assembly resolution 55/25 of 15 November 2000, and it is the main international instrument in the fight against transnational organized crime

CTF (Countering the Financing of Terrorism): This term involves the use of funds that may be licit or illicit in origin and using these funds to support terrorist activity.

Customer Risk Rating Assessment: They are one of three primary tools used by financial institutions to detect money laundering. The models deployed by most institutions today are based on an assessment of risk factors such as the customer's occupation, salary, and the banking products used.

Digital Payment Token: It refers to any cryptographically secured digital representation of value that is used or intended to be used as a medium of exchange.

FATF (Financial Action Task Force): It is an intergovernmental institution created in 1989 by the then G8. The purpose of the FATF is to develop policies to help combat money laundering and terrorist financing.

Financial Intelligence Units (FIUs): Investigative units established by individual countries to centralize the gathering of suspicious activity reports related to criminal financial activity and sharing the results of the analysis with relevant government agencies.

KYB (Know Your Business): These strategies focus on establishing optimal relationships with other companies that may be customers or suppliers, to mitigate the risk of doing business with an untrustworthy entity or one that has been involved in a compromising situation in the past.

KYC (Know Your Customer): These procedures are established around a process of identification and verification of a customer's identity in which a series of controls and checks are applied to prevent business relationships with persons linked to terrorism, corruption or money laundering.

KYS (Know Your Supplier): This practice provides more insights and transparency on suppliers and related supply chain risks, in order to address topics such as supplier performance, business continuity, sustainability, fraud & bribery, security risk, money laundering, child labor, and other legal/organizational compliance requirements.

Lines of Defense Model: The three lines of defense represent an approach to providing structure around risk management and internal controls within an organization by defining roles and responsibilities in different areas and the relationship between those different areas.

Money Mule: A person who transfers or moves illegally acquired money on behalf of someone else.

Peep Screening: It is a process that aims to identify and conduct customer due diligence on any politically exposed person as part of a robust Anti-Money Laundering and Know Your Customer (AML/KYC) program.

PEP: Politically Exposed Person.

Sanction Screening Program: is a combination of policies, procedures and technologies that enable a financial institution to ensure that it does not provide any form of services to sanctioned parties, directly or indirectly.

Transaction Monitoring Program: It helps financial institutions automatically spot suspicious transactions, such as high-value cash deposits or unusual account activity.

References

Basel Committee on Banking Supervision. (2013). Principles for effective risk data aggregation and risk reporting.

Board of Governors of the Federal Reserve System (2018). Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing. https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms

Board of Governors of the Federal Reserve System (2021). Request for Information and Comment on financial institutions' Use of Artificial Intelligence, Including Machine Learning. https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence

European Banking Authority. (2021). Guidelines on cooperation and information exchange between prudential supervisors, AML/CTF supervisors and financial intelligence units under Directive 2013/36/EU.

European Commission. (2019). https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:52019DC0373

European Commission. (2019). Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions.

European Parliament and the Council. (2015). Directive (EU) 2015/849.

European Banking Authority. (2019). Opinion of the European Banking Authority on communications to supervised entities regarding money laundering and terrorist financing risks in prudential supervision.

European Banking Authority. (2021). Final report on draft regulatory technical standards under Article 9a (1) and (3) of Regulation (EU) No 1093/2010.CTF.

European Banking Authority. (2021). Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector.

European Banking Authority. (2021). Guidelines on the use of remote customer onboarding solutions.

European Banking Authority. (2022). Guidelines on the role of AML/CTF compliance officers.

European Parliament. (2021). Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets (recast).

Europol. (2018). Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain. https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain#downloads

Lexis Nexis Risk Solutions (2021). Global cost of compliance.

European Parliament. (2021). Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010.

Federal Deposit Insurance Corporation (2021). Appendix 1010.230 Beneficial ownership requirements for legal entity customers. FDIC Law, Regulations, Related Acts.

Financial Conduct Authority. FCA Handbook. https://www.handbook.fca.org.uk/handbook/glossary/G416.html

Financial Action Task Force. (2013). National Money Laundering and Terrorist Financing Risk Assessment.

Financial Action Task Force. (2014). Virtual Currencies Key Definitions and Potential AML/CTF Risks.

Financial Action Task Force. (2019). FATF Ministers give FATF an open-ended Mandate.

Financial Conduct Authority (2022). Regulatory Sandbox accepted firms. https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms

Financial Crimes Enforcement Network. (2020). The Anti-Money Laundering Act of 2020.

Financial Services Agency. (2021). Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism.

Holman, D.; Stettner, B. (2018). Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches. Allen & Overy, LLP.

L. Alsedà, A. Awasthi, Jörg Lässig (2012): Genetic Clustering Algorithms for Detecting Money-Laundering. 2012.

Monetary Authority of Singapore. (2021). Consultation Paper on Proposed AML Notices for Cross-Border Business Arrangements of Capital Markets Intermediaries under Proposed Exemption Frameworks.

Mersch, Y. (2019). Anti-money laundering and combating the financing of terrorism – recent initiatives and the role of the ECB. https://www.bankingsupervision.europa.eu/press/speeches/date/2019/html/ssm.sp191115~a435dd398e.en.html

Paesano, F. (2021). Cryptocurrencies and money laundering investigations. Basel Institute on Governance.

People's Bank of China. (2021). Measures for the Supervision and Administration of Anti-Money Laundering and Anti-Terrorist Financing of financial institutions.

Republic of Singapore. (2019). Payment Services Act.

Sanction Scanner. (2021). Anti-Money Laundering (AML) Fines of 2021. https://sanctionscanner.com/blog/anti-money-laundering-aml-fines-of-2021-561

Soltani, R.; Nguyen, U.; Yang, Y.; Faghani, M. (2013). A new algorithm for money laundering detection based on structural similarity.

The Institute of International Finance; Deloitte. (2021). The effectiveness of financial crime risk management reform and next steps on a global basis.

United Nations Office on Drugs and Crime. Money Laundering. https://www.unodc.org/unodc/en/moneylaundering/overview.html

United Nations Office on Drugs and Crime. (2005). UN Convention Against Transnational Organized Crime and the Protocols Thereto.

United Nations Office on Drugs and Crime (2011). Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes. Research report. October 2011.

Weber, M; Chen, J.; Suzumura, T.; Pareja, A.; Ma, T.; Kanezashi, H., Kaler, T.; Leisersen C.E.; Schardl, Tao B. (2018). Scalable Graph Learning for Anti-Money Laundering.

World Economic Forum. Global Coalition to Fight Financial Crime. https://www.weforum.org/projects/coalition-to-fight-financial-crime

HM Treasury: National risk assessment of money laundering and terrorist financing. December 2020.

Our aim is to exceed our clients' expectations, and become their trusted partners

Management Solutions is an international consulting services company focused on consulting for business, risks, organization and processes, in both their functional components and in the implementation of their related technologies.

With its multi-disciplinary team (functional, mathematicians, technicians, etc.) of more than 3,300 professionals, Management Solutions operates through its 41 offices (17 in Europe, 20 in the Americas, 2 in Asia, 1 in Africa and 1 Oceania).

To cover its clients' needs, Management Solutions has structured its practices by sectors (Financial Institutions, Energy, Telecommunications and other industries) and by lines of activity, covering a broad range of skills -Strategy, Sales and Marketing Management, Risk Management and Control, Management and Financial Information, Transformation: Organization and Processes, and New Technologies.

The R&D department provides advisory services to Management Solutions' professionals and their clients in quantitative aspects that are necessary to undertake projects with rigor and excellence through the implementation of best practices and the continuous monitoring of the latest trends in data science, machine learning, modeling and big data.

Juan G. Cascales
Partner at Management Solutions
juan.garcia.cascales@msunitedkingdom.com

Antonio Tazón
Partner at Management Solutions
antonio.tazon@msnorthamerica.com

Patricia Pajuelo
Director at Management Solutions
patricia.pajuelo@msnorthamerica.com

Luke Harrison
Experienced Senior at Management Solutions
luke.harrison@msunitedkingdom.com

Management Solutions, Professional Consulting Services

Management Solutions is an international consulting firm whose core mission is to deliver business, risk, financial, organization, technology and process-related advisory services.

For further information please visit **www.managementsolutions.com**

Follow us at:

www.managementsolutions.com

Madrid Barcelona Bilbao Coruña London Frankfurt Düsseldorf Paris Amsterdam Copenhagen Oslo Warszawa Zürich Milano Roma Bologna Lisboa Beijing Istanbul Johannesburgo Sydney Toronto New York New Jersey Boston Pittsburgh Atlanta Birmingham Houston San Juan de Puerto Rico San José Ciudad de México Monterrey Querétaro Medellín Bogotá Quito São Paulo Lima Santiago de Chile Buenos Aires