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 – SAR). 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.

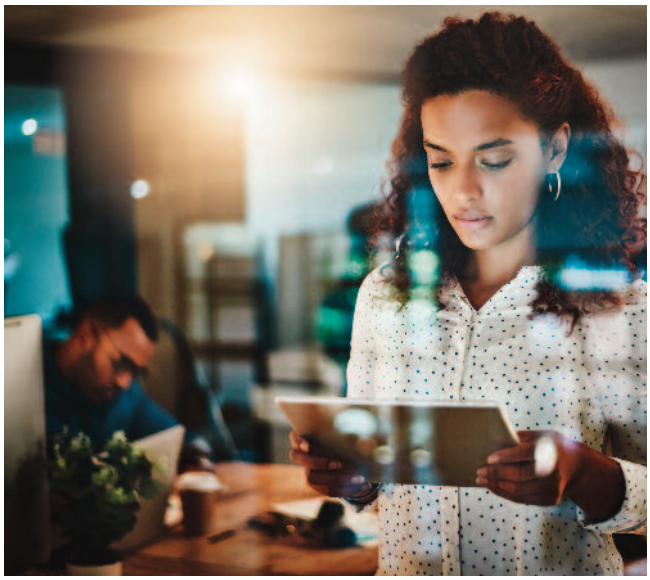
27. ***Data management capabilities.*** These demands on data require the development of Data Management capabilities. One of them is a Data Quality capability to proactively specify business rules and data quality standards around critical data, and then systematically measure those rules to identify 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 Compliance Management 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 (ARPA). 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. ARPA 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 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.