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 agencies[14]. The 5th EU AML Directive[15] required an

[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). , , 09.07.2018, p.1.
[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

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). CTF
[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). Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU.
[21] Financial Conduct Authority (2022). Regulatory Sandbox.