2. Executive summary

2.1 Background

Money laundering is a global problem that undermines the integrity and safety of the global financial system. Currently, financial institutions monitor transactions for suspicious activities in a siloed way. However, this approach is ineffective as many payment transactions are complex and involve interconnected networks that span multiple financial institutions and borders. Criminals operate in networks and exploit this complexity.

Both legitimate and illicit transactions flow through payment systems. A network view of payments data is essential to combat money laundering.

Financial institutions are exposed to increasing levels of various types of financial crimes, with 67% exposed to financial crimes involving digital payments and over 60% to various forms of money laundering.[1] The amount of money laundered globally is estimated to be between 2 and 5% of global GDP, or between $2 trillion and $5 trillion.[2] However, the estimated total sum seized annually amounts to less than 1% of this – between $20 billion and $50 billion.[3]

A 2022 study found that financial institutions face compliance costs of approximately $274 billion globally,[4] an increase of approximately 28% on the 2020 figure of approximately $214 billion.[5] Between 2019 and 2022, the average costs of compliance grew by approximately 54% in the United States, 80% in Canada, 30% in Germany and 23% in France.[6, 7]

When asked about the major factors driving compliance costs, increasing anti-money laundering (AML) regulation was cited by 68% of financial institutions, while another 68% cited evolving criminal threats.[8] These factors combined with the risk of sanction, have contributed to a defensive approach to AML compliance being adopted by financial institutions. This defensive approach can lead to over-reporting to authorities, which can become a drain on public resources. It can also result in the

[1] See Lexis Nexis (2022).

[2] See UNODC. The source states $800 billion to $2 trillion based on global GDP at the time of writing. When the estimated value laundered is calculated based on global GDP in 2022, which was approximately $100 trillion (see Statista 2023), the estimated value laundered would be between $2 trillion - $5 trillion. It should be noted that it is difficult to estimate the total amount of money that goes through the laundering cycle.

[3] See Statista (2023). The value for the total sum seized is calculated from the estimated value laundered based on global GDP in 2022, which was approximately $100 trillion.

[4] See Lexis Nexis (2022).

[5] See Lexis Nexis (2021).

[6] See Lexis Nexis (2022).

[7] See Lexis Nexis (2021).

[8] See Lexis Nexis (2022).

termination of customer relationships to reduce overall exposure to financial crime risk (known as "de-risking").[9]

2.2 Data, technology and innovation

In response to some of these challenges, the Financial Action Task Force (FATF) has identified that data-sharing and collaborative analytics are critical for effective anti-money laundering and countering the financing of terrorism (CFT) efforts.[10] In its *Stocktake on data pooling, collaborative analytics and data protection*,[11] the FATF outlined several technologies and approaches that could be used to improve AML/CFT efforts, including different approaches to data-sharing,[12] privacy-enhancing technologies (PET),[13] advanced analytics,[14] data standardisation[15] and data protection.[16] Digital transformation to enhance AML/CFT efforts is a strategic priority of the FATF.[17]

Additionally, in 2020, the G20 leaders endorsed a *Roadmap for enhancing cross-border payments*. As part of this roadmap's prioritisation plan, the FATF is also considering updating its recommendation 16 (the travel rule)[18] to take into account developments in the architecture of payment systems, including the adoption of ISO 20022 messaging standards. This is to improve the consistency and usability of payment message data in cross-border payments and could also facilitate more efficient AML/CFT checks.

Technology and collaboration could support financial institutions, central banks, supervisory and other public authorities to address AML challenges through collaborative analytics and learning (CAL). Such initiatives could leverage payment system-level data and public-private collaborative approaches to analyse privacy protected data[19] to reveal suspicious networks and activities that may not be detected by financial institutions acting in isolation.

[9] See FATF (2021a).

[10] See FATF (2021a).

[11] See FATF (2021b).

[12] Sharing information could also support customer due diligence measures such as institutional risk assessment, customer onboarding, risk management of a business relationship, identification of the beneficial owner, and could help identify and share patterns and flows, such as typologies.

[13] Privacy-enhancing technologies (also referred to as cryptography/encryption technologies) such as homomorphic encryption, secure multi-party computation, differential privacy and zero-knowledge proofs can facilitate secure and privacy-protected information-sharing and analysis.

[14] Advanced analytics such as machine learning, federated learning, deep learning, network analysis and natural language processing can be applied to analyse large amounts of structured and unstructured data more efficiently, and identify patterns and trends more effectively.

[15] See FATF (2021a).

[16] See FATF (2021b).

[17] See FATF (2022).

[18] See FSB (2022).

[19] Collaborative approaches to analysis include centralised, decentralised or hybrid (centralised and decentralised) at a national and cross-border level. These are discussed further in section 4.4.

The protection of individual and fundamental rights to privacy can be a concern when considering the use of data and technologies to fight financial crime. Data privacy and protection, and countering financial crime are important public interests that are not opposed to each other. They should be supported by the right technological tools and by a balanced legal framework.

2.3 Project Aurora

Project Aurora builds upon the above-mentioned initiatives and challenges in a proof of concept (PoC). The PoC investigates the use of privacy-enhancing technologies and advanced analytics for different CAL approaches for detecting money laundering activities. The PoC contains the following parts:

- Generation of a synthetic data set that represents transactions between financial institutions, individuals and businesses within a country and across borders. The data set also reflects complex money laundering events that are embedded in the data. The data set consists of a minimum set of data fields, which are common to different payment ecosystems, such as instant payment systems (IPS) and potential CBDC systems, as well as data fields required in any CAL arrangements.

- Testing three different simulated monitoring scenarios (views the synthetic data at the single financial institution level, at the national level and at the cross-border level) with machine learning models[20] and network analysis to compare the performance[21] of the scenarios in detecting money launderers and suspicious networks.

- Testing and comparing the performance of different CAL approaches – such as centralised, decentralised or hybrid at the national and cross-border levels – in detecting money launderers and suspicious. Privacy-enhancing technologies were applied to the data in each approach and analysed using advanced analytical methods to examine how privacy-enhancing technologies could support privacy and data protection.

2.4 Key findings and takeaways

Project Aurora demonstrates the advantages and potential of using payments data in combination with privacy-enhancing technologies, machine learning models and network analysis for the detection of complex money laundering schemes. The project also simulates how these data and technologies could be brought together to enable public-private collaborative analysis and learning (CAL) arrangements, both nationally and internationally, to counter money-laundering. The project demonstrates that **CAL**

[20] Machine learning is a subset of artificial intelligence. It enables a machine to learn from insights from the data. Machine learning is used in this report refers to "artificial intelligence and machine learning".

[21] Performance is made up of two parts: effectiveness and efficiency. These refer to the fraction of money laundering activities detected in the data while keeping the number of false positives low.

approaches are more effective in detecting money laundering networks than the current siloed approach (in which financial institutions carry out analysis in isolation).

2.4.1 A holistic view of payments data unveils money laundering networks

A **holistic view of payments** data is essential to effectively identify and combat suspicious activities that take place beyond the bounds of single financial institutions and national borders. Leveraging these data could lead to improvements in monitoring by opening up a holistic view on transaction networks that unveil money laundering networks.

At a national level, the analysis approaches explored in this project could be performed via transaction monitoring utilities or CAL arrangements in which different ecosystems of payments data (eg financial institutions, fintech, virtual asset service providers (VASPs), card schemes, e-money or others) are connected. At a cross-border level, similar analysis could take place in a CAL arrangement.

Similarly these approaches could be used by operators (eg central banks or private sector entities) of **IPS or potential CBDC** systems that include AML monitoring and analysis capabilities. Operators of these systems could provide participants with additional tools and support to enhance their monitoring efficiency.[22]

2.4.2 Behavioural monitoring and privacy enhancing technologies could be a game changer for AML efforts

Utilising network analysis for detecting anomalous and suspicious networks shifts the focus from individual behaviour to the overall behaviour of suspicious networks, resulting in improved detection capabilities.

Project Aurora demonstrates the potential to improve the detection of money laundering while reducing the number of incorrect alerts. Furthermore, the project shows that the optimal performance of machine learning models is observed in a simulated cross-border scenario in which sensitive transaction data are protected and secured (using encryption or a combination of privacy preserving methods), consolidated into a centralised system[23] and where network analysis is utilised.

Moreover, a centralised approach that consolidates privacy-enhanced transaction data at a national level and collaborates with other countries to collectively train a machine learning model (in a decentralised approach using federated learning) that

[22] There could be limitations on the types of money laundering activities and actors that could be detected depending on design choices and data available. Section 5.1.1 discusses this further.

[23] While Project Aurora simulated a centralised cross-border CAL approach in the experiment, it should be noted that in reality the challenges associated with data protection, data localisation, legal, regulatory and other factors would be complex. A decentralized CAL approach using federated learning at a cross-border level may offer an alternative solution, however there could be a trade-off with effectiveness in detecting money laundering activities.

can be applied locally, could support potential cross-border collaboration on AML efforts, while upholding the data sovereignty of individual countries. [24]

2.4.3 Leveraging Project Aurora

To leverage Project Aurora, three aspects should be kept in mind:

First, the specific data fields and sources required for detection of financial crime may vary depending on the techniques and methods used by criminals. It is essential to have a thorough understanding of different types of financial crimes and identify the data fields and sources that may help indicate their occurrence. Project Aurora shows that the performance of such analysis is only as good as the breadth of data available. Data quality and standardisation of data identifiers and fields are important factors.

The adoption of ISO 20022 could be an opportune moment to catalyse greater international consistency in the use of data identifiers and fields, and their shared definitions (available in machine readable form), that could be used for financial crime detection and to enable CAL arrangements. For example, the inclusion of the legal entity identifier (LEI) in ISO 20022 payments messages. When combined with the additional data fields available in these messages, the LEI could help identify a greater range of money laundering activities involving legal entities.[25] Similarly, standards being developed for identification of beneficial owners, would be important too. These standards are further discussed in Annex A.

Second, further discussion on the public benefits of CAL arrangements for AML followed by legislative clarity to support such arrangements would be necessary. Data protection agencies should be engaged at an early stage to be part of co-design processes with other stakeholders in CAL arrangements to identify and mitigate risks and address uncertainties, for example considering the role and application of PETs.

Third, effective CAL arrangements, as a public-interest tool for financial crime detection, as part of a broader strategic framework for financial crime prevention and disruption, would require collaboration between the public and private sectors to contribute to and deliver such a strategic approach. Any such approach would need to consider the prioritisation of risks and responses to them, the data required, trust between participants and the legal certainty needed to enable a CAL arrangement. National strategies for AML monitoring and analysis could also include the appropriate cross-border CAL initiatives to gain a broader view of money laundering networks and the flow of funds.

It takes a network to defeat a network.

[24] See The White House (2021): the US and UK prize challenge to advance privacy-enhancing technologies as they present an opportunity to leverage the power of data while protecting privacy and intellectual property, and enable cross-border and cross-sector collaboration.

[25] The legal entity identifier (LEI) is the global standard for legal entity identification. It could enable data associated to legal entities to be linked to transaction data within and across borders. The LEI could connect a greater range of data sets and capture different relationships which could be useful in AML efforts. It could also address the challenges faced by monitoring systems from inconsistencies in how entities are identified.