FATF

STOCKTAKE ON DATA POOLING, COLLABORATIVE ANALYTICS AND DATA PROTECTION

JULY 2021

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2021), *Stocktake on Data Pooling, Collaborative Analytics and Data Protection,* FATF, Paris, France, https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html

Photocredits coverphoto: Gettyimages

Acknowledgements

The FATF would like to thank public and private sector stakeholders—including technology developers, financial institutions and data protection authorities—for providing valuable input, case studies and feedback to this report.

The work of this report was led by the FATF Secretariat (Kristen Alma), with significant input provided by a Group of Experts from the following FATF delegations: Canada, European Commission, France, Germany, Israel, Italy, Japan, MONEYVAL Secretariat, the Russian Federation, Singapore, Switzerland, United Kingdom, United Nations, and the United States.

Table of contents

Acronyms 3

Executive Summary 4

1. Introduction 5

2. Methodology 7

3. Background 8

4. Objectives and Preconditions for Private Sector AML/CFT Information Sharing and Analysis 10

4.1. Why share data? 10
4.2. What are the stated goals for private-to-private data pooling initiatives? 12
4.3. What type of data could be shared? 13
4.4. Drivers and preconditions for the use of new technologies 15

5. New Technologies Identified to Share and Analyse AML/CFT Information 21

5.1. Identified technologies for private-to-private information sharing 21

6. Challenges related to the use of new technologies for data collaborative analytics 26

6.1. Ensuring and Enhancing Data Protection and Privacy 27
6.2. Data Quality 32
6.3. Lack of Regulatory Clarity 32
6.4. Explainability and Interpretability 33
6.5. STR Confidentiality and Tipping Off 34
6.6. Market Structure and Competition 35
6.7. Technology Costs and Constraints 35
6.8. Defensive Reporting and De-risking 36
6.9. Security 37
6.10. Avoidance of Analytical Bias in Artificial Intelligence 37
6.11. Human Rights 37

7. Enabling the wider use of data pooling and advanced analytics 38

7.1. Regulatory Clarity 38
7.2. Promotion of Enabling Environments 38
7.3. Data Standardisation and Governance 39
7.4. Bias Prevention in Artificial Intelligence 39

8. Concluding Remarks 41

Annex A. Glossary 42

Annex B. Additional Regtech Cases Studies on New Technologies for Private-to-Private AML/CFT Data Sharing and Analysis. 47

Annex C. Suggested Actions to Support the Use of Technology in AML/CFT 49

References 51

Acronyms

AI	Artificial intelligence
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
API	Application Programming Interface
CDD	Customer Due Diligence
DL	Deep Learning
DLT	Distributed Ledger Technology
DNFBP	Designated Non-financial Business and Profession
DPP	Data Protection and Privacy
EDPB	European Data Protection Board
FATF	Financial Action Task Force
FI	Financial institution
GDPR	General Data Protection Regulation
MER	Mutual Evaluation Report
ML/TF	Money Laundering/Terrorist Financing
MVTS	Money or Value Transfer Service
NLP	Natural Language Processing
NRA	National Risk Assessment
PEP	Politically Exposed Person
PSCF	Private Sector Consultative Forums
SSB	Standard Setting Body
STR	Suspicious Transaction Report

Executive Summary

1. Recent technological advances help financial institutions analyse large amounts of structured and unstructured data more efficiently and identify patterns and trends more effectively. By pooling data and using collaborative analytics, financial institutions can better understand, assess, and mitigate money laundering and terrorist financing risks. This will result in a more dynamic, effective and efficient identification of these activities, and help the private sector comply with anti-money laundering and counter terrorist financing requirements in a timelier and less burdensome manner. It can also help prevent criminals from exploiting information gaps as they engage with multiple domestic and international financial institutions to launder their illicit funds, each having a limited and partial view of transactions.

2. However, data pooling and collaborative analytics also have the potential to infringe on the protection of individual and fundamental rights to privacy. Therefore, it is imperative that any exchange of information respects national and international data protection and privacy legal frameworks.

3. This report acknowledges that AML/CFT and data privacy and protection are both significant public interests that serve important objectives. These objectives are neither in opposition nor inherently mutually exclusive. Data protection principles and rules through international and domestic legal instruments aim to protect human rights and fundamental freedoms, notably the right to privacy. This report notes that it is essential that legal regimes facilitate both of these objectives, in order to prevent money laundering, terrorist financing, proliferation financing, and other financial crimes, in a way that respects individuals' fundamental rights to privacy and data protection.

4. New and emerging privacy-enhancing technologies offer promising ways to protect information in specific use cases and in line with national and international data protection and privacy frameworks. Privacy-enhancing technologies rely on a range of different cryptographic tools to enable privacy in various applications. These tools enable multiple parties to interact meaningfully to achieve an application goal, without revealing underlying private information to one another or to third parties. There is a growing field of research and discussion on this subject, but there are not yet any technical standards. Much work remains to develop such standards and open source references, which will clarify the specific use-cases where privacy-enhancing technologies can protect data privacy.

5. This stocktake report examines commercially available and emerging technologies that facilitate advanced AML/CFT analytics within individual regulated entities and collaborative analytics between them. This report also includes an analysis of the intended objectives and drivers for the use of these new technologies. It also identifies policy considerations and potential solutions when considering or deploying such technologies.

6. The FATF will continue its dialogue between AML/CFT supervisors, technology developers, financial institutions, and data privacy and protection authorities, and other relevant experts. This will ensure that new technologies that can improve AML/CFT effectiveness are fully utilised, consistent with data privacy and protection national and international frameworks.

1. Introduction

7. Data pooling and collaborative analytics, refers to a process where (digital) data from different sources are analysed (including by multiple parties). These pools may be organised in a centralised (data pooling) or a distributed way (collaborative analytics).[1] This paper addresses data pooling and collaborative analytics between financial institutions (FIs), including within and outside international financial groups. Data pooling and collaborative analytics carry benefits but also some significant risks. It may enable the use of analytical tools that have the potential to strengthen the shared understanding, assessment and mitigation of money laundering (ML) and terrorist financing (TF) risks, resulting in a more dynamic, effective and efficient identification of these activities. It can reduce the number of false positives, enabling more effective compliance by the private sector in a timelier and less burdensome manner. It can also help prevent the exploitation of information gaps that enable regulatory arbitrage by criminals, who may attempt to engage with multiple domestic and international FIs, each having a limited and partial view of transactions. However, it may also infringe on the protection of individual and fundamental rights. Therefore, it is imperative that any exchange of information respects national and international data protection and privacy (DPP) legal frameworks.

8. Technological advances in recent years allow FIs to analyse large amounts of structured and unstructured data more efficiently and identify patterns and trends more effectively. The use of big data and advanced analytics, such as artificial intelligence (AI)[2], has the potential to enhance AML/CFT compliance in the financial sector, but comes with risks to fundamental and individual rights when personal data is shared or the processes lack adequate explainability and may produce biased or otherwise erroneous results. For example, FIs could leverage advanced analytics to more accurately identify suspicious activities, screen their customers, and manage risks. Since the accuracy of advanced analytics largely corresponds to the size, quality and relevancy of the data set, the efficacy and efficiency of these tools may depend on the ability of FIs (within and outside of financial groups) to share information.

9. Technologies that exchange, pool, or analyse data must protect personal information in line with national and international legal frameworks. The need for data sharing thus requires careful analysis of both the AML/CFT and DPP implications. For example, FIs should only collect and process personal data that is necessary (i.e., data minimisation) to fulfil a specific and defined purpose (i.e., purpose limitation) and not further process in a manner incompatible with those purposes. Information should also be shared to achieve a certain aim that cannot be achieved through less invasive measures requiring less access to personal identifiable information. Collected data should also not be retained for longer than

[1] For collaborative analytics, data is not moved to a central location in order to analyse them together with other data assets. Instead, the analytical tools come to the data, not the other way around. This makes it easier to keep the data secure and to ensure control over who accesses what data for what purposes.

[2] See Annex A for a list of Key Digital Transformation Definitions.

necessary and should not be transferred to an entity that does not have compatible data protection rules.

10. New and emerging privacy-enhancing technologies offer promising ways to protect information in specific use cases and in line with national and international DPP frameworks. Privacy-enhancing technologies rely on a range of different cryptographic tools for enabling privacy in various applications.[3] These tools are intended to enable multiple parties to interact meaningfully to achieve an application goal, without revealing underlying private information to one another or to third parties. While there is a growing field of research and discussion on this subject, technical standards have not yet been created and there is much work to be done to develop standards and open source references to provide clarity as to whether privacy-enhancing technologies provide data privacy protections in specific use cases. Moreover, when the aim of such technologies is to use data to identify a specific natural or legal person (e.g., customer on-boarding), data privacy protections may be impaired. Therefore, data sharing initiatives in some jurisdictions may currently be limited to sharing non-personal data (e.g., corporate data excluding customer-related data) that falls outside the scope of relevant DPP legal requirements.

11. In June 2020, in line with the German FATF Presidency priorities related to AML/CFT Digital Transformation, the FATF agreed to conduct a stocktake on Data Pooling, Collaborative Analytics and Data Protection. The purpose of this project is to examine commercially available or emerging technologies that facilitate advanced AML/CFT analytics within regulated entities or collaborative analytics between FIs, and to identify challenges and potential solutions so that this technology may be fully utilised to strengthen AML/CFT compliance, consistent with DPP national and international frameworks.

12. This stocktake report is organised as follows: Section 2 provides a background on the FATF's previous work on private sector data sharing; Section 3 outlines the intended objectives and drivers for the use of new technologies for private sector data sharing and analysis; Section 4 summarises the various new technologies under development or in use; Section 5 lists the challenges and obstacles Questionnaire respondents encountered while developing or deploying these technologies; and Section 6 outlines respondents' proposed solutions to the wider deployment of new technologies (which are not presently endorsed by the FATF).

13. Regarding this project's scope, this paper examines private-to-private data pooling and collaborative analytics (including efforts supported or initiated by public authorities). The use of new technologies for public-private information sharing—in particular, between reporting entities and financial intelligence units/law enforcement agencies—is examined under a separate paper on Digital Transformation of AML/CFT for Operational Agencies.

[3] Privacy-enhancing technologies include: homomorphic encryption (HE), Fully-Homomorphic Encryption (FHE), Zero-knowledge proofs (ZKP), Secure multiparty computation (SMPC), functional encryption (FE), Group and ring Signatures (GRS), Private Information Retrieval (PIR), Private Set Intersection (PSI), Searchable Encryption (SE), Blind signatures (BS), https://csrc.nist.gov/CSRC/media/Projects/pec/documents/suite-draft1.pdf; identity-based encryption (IBE), etc. See, e.g., https://csrc.nist.gov/projects/pec; https://csrc.nist.gov/CSRC/media/Presentations/icmc2020-slides/images-media/20200923-PEC-ICMC-slides.pdf; https://zkproof.org/.

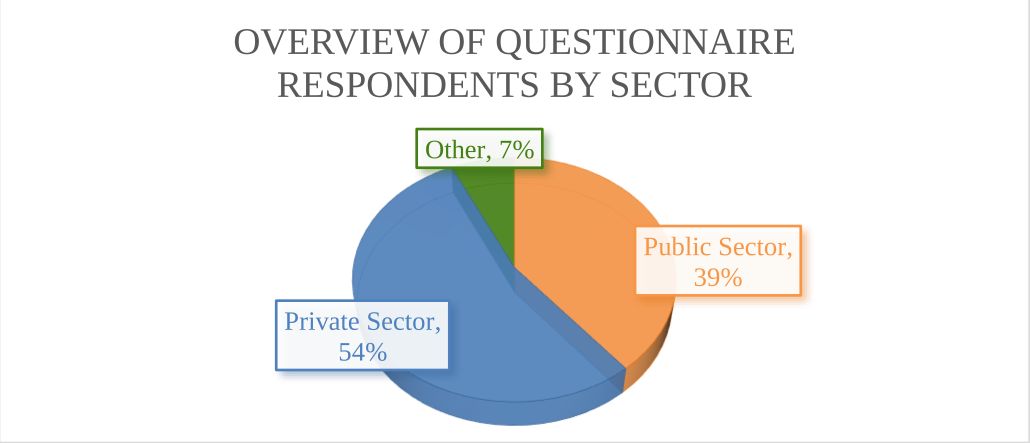
2. Methodology

14. In November 2020, the FATF circulated an online Questionnaire on Digital Transformation to AML/CFT national authorities and private sector stakeholders (including academia, FIs and technology developers), to identify the various new technologies available to facilitate collaborative analytics. In total, 188 completed responses were received. This paper summarises the results of this Questionnaire, as well as desk-based research and interviews with public and private sector stakeholders, including representatives from FIs, technology developers, and AML/CFT and DPP authorities.

15. The questionnaire gathered stakeholders' views on the intended results of using new technologies to facilitate collaborative analytics, but also how new technologies are being used in an attempt to secure, collaborate and analyse data. It also included questions on the challenges and policy considerations related to the implementation of such technologies, and engagement with AML/CFT and DPP supervisors. The questionnaire also sought case-studies to illustrate good practices by "respondents" (hereinafter referring to those who responded to the Questionnaire and experts contacted by the Secretariat, including experts nominated from FATF delegations).

16. The breakdown of responses per sector is shown in the chart below. At the public sector level, the majority of respondents classify as supervisors, whereas at the private sector level the majority of input came from FIs and technology developers.[4] Institutions classified as "large banks" were the main contributors to the questionnaire. The majority of respondents are based in Europe (53%), followed by Americas (20%), Asia/Oceania (18%), and Africa (9%).[5]

Figure 1. Overview of Questionnaire Respondents by Sector



[4] Of those respondents who specified as "private sector", 54% specified as "financial institutions", and 46% specified as "technology providers".

[5] "Other" respondents specified as non-profit organisations, think tanks and academics.

3. Background

17. Data pooling and collaborative analytics is not an entirely new topic to the FATF. Some of the FATF's Recommendations include elements related to private-to-private information sharing. For example, Recommendation 18 requires information sharing within the context of financial groups for customer due diligence (CDD) purposes and ML/TF risk management. Such sharing includes information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include a suspicious transaction report (STR), its underlying information, or the fact that an STR was submitted. This requirement applies to all the entities (in domestic and cross border environments) captured by the definition of financial group in the FATF Glossary.[6] Recommendation 21 further ensures that FIs and their directors, officers and employees are able to disclose the fact that an STR or related information has been submitted so long as it is pursuant to group-wide ML/TF risk management requirements as set out in Recommendation 18. Finally, the measures under Recommendation 2 – requiring authorities to cooperate and coordinate to ensure the compatibility of AML/CFT requirements with DPP and other similar provisions – highlight the important role that authorities play in addressing impediments to information sharing, actual or perceived.

18. While these recommendations outline the parameters for information sharing in the financial group context, the FATF Standards do not presently include similar requirements for information sharing outside of the financial group.

19. In 2017, the FATF published its Guidance on Private Sector Information Sharing. The Guidance highlights initiatives in information sharing amongst FIs that go beyond the FATF Recommendations (page 22-25). Since then, there have been a number of regional/national initiatives in this area. For example, the non-binding recital 46 to the fifth Anti-Money Laundering Directive of the European Union (EU) articulates, *"criminals move illicit proceeds through numerous financial intermediaries to avoid detection. Therefore it is important to allow credit and financial institutions to exchange information not only between group members, but also with other credit and financial institutions, with due regard to data protection rules as set out in national law."*[7] In December 2020, the European Data Protection Board (EDPB) also adopted a statement noting, *inter alia*, that the upcoming update to the legislation[8] is an opportunity to address the interplay between the protection of privacy and personal data and AML/CFT measures, as well as their concrete application on the ground. The EDPB notes that it is convinced that a closer

[6] The FATF Glossary defines Financial Group as "a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level".

[7] Recital 46 to Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[8] EU plans a single rulebook in the form of a harmonising regulation on AML.

articulation between the two sets of rules [AML/CFT and DPP] would benefit both the protection of personal data and the efficiency of the AML framework. The EDPB reiterated the need for a clear legal basis for the processing of personal data and stating the purposes and the limits of such processing, in line with Article 5(1) General Data Protection Regulation (EU GDPR), in particular regarding information sharing and international transfers of data. (EDPB, 2020,[1])

20. With the introduction and application of various privacy enhancing technologies[9], a number of initiatives and pilot programs have been launched by the private sector to pool and collaboratively analyse data, including CDD data, to enhance AML/CFT compliance and better identify illicit activity. These international initiatives highlight the appetite amongst FIs to collaborate and pool resources, and the need for the FATF to go further than the existing guidance, in order to address data pooling and collaborative analytics in the context of new technology.

[9] Privacy enhancing technologies (often referred to as PETs or privacy-enhancing cryptography), are "Specialist cryptographical capabilities, which allow computations to take place on underlying data, without the data owner necessarily divulging that underlying data. The same technology can ensure that the data owner does not have visibility over the search query, with the query and the results remaining encrypted (or not disclosed) and only visible to the requester." (Maxwell, 2020[16])

4. Objectives and Preconditions for Private Sector AML/CFT Information Sharing and Analysis

21. The FATF recently examined information sharing within and between FIs and financial groups in the narrower context of sharing specific information on a case-by-case basis for AML/CFT purposes (e.g., to review a customer that has triggered a red-flag indicator). This stocktake report builds upon that work by considering how technological innovations that rely on large-scale private-to-private data pooling and collaborative analytics can facilitate AML/CFT/CPF objectives, while also respecting DPP requirements.

22. Emerging technologies tested in other domains that involve the encryption of sensitive personal data, such as in the health sector[10] may offer innovative solutions to respect diverging national and international DPP laws and allow for the exchange and analysis of information for AML/CFT purposes. Indeed, according to the results of the Questionnaire, 93% of respondents believe that new technologies may help overcome these and other data sharing challenges in AML/CFT (e.g., protection of proprietary information for competitive purposes).

4.1. Why share data?

23. Data sharing is critical for combatting ML, TF and the financing of proliferation (PF). Multinational ML/TF/PF schemes do not respect national boundaries, nor do criminals exploit only one institution to launder their ill-gotten gains. Oftentimes, illicit activity only becomes apparent when institutions and authorities can examine aggregated activity of an actor across different borders and platforms. This is evidenced by the various international laundromat cases that exploited weaknesses in FIs across multiple jurisdictions in order to launder significant proceeds of crime. Coordinated assessments of aggregated activity by multiple institutions may improve the overall quality of financial intelligence developed.

24. In order to better prevent and detect the abuse of the international financial system for ML/TF purposes, FIs could consider collaborating if and where it is compliant with DPP requirements within a financial group, and between FIs that are not part of the same financial group. At the same time, FIs should be conscious of liability they may incur for the breach of DPP requirements. Generally, FIs are not recommended to share personal data unless the parameters of such data sharing (types of data, circumstances for sharing, communication channels, etc.) are explicitly prescribed by legislation of the jurisdiction of their operation.

25. Such sharing of information may be supported by authorities but could equally occur at the industry level, and does not necessarily require governmental involvement, as long as the parameters and purpose for data collaboration are clearly defined by law, and there is effective data protection oversight over private sector implementation.

26. Respondents noted that gaining access to a wider set of data could improve outcomes and enable intelligence-led decision making by reducing false positives,

[10] For example, the use of federated data (or federated learning) is a growing trend in the health sector to facilitate information sharing and research collaboration (Tim Hulsen, 2020[19])

driving prioritisation, advancing the efficiency of financial crime investigations, improving enterprise data quality, and enabling greater operational efficiency. Of course, data quality and data standardisation are important elements to the overall accuracy of collaborative analytics, as outlined in section 6.2.

27. Advanced analytics applied to data shared by multiple FIs can reveal trends or potentially suspicious activities that could otherwise go undetected by a sole institution. For example, respondents noted that tools and techniques such as entity resolution and network analysis allow links to be identified, which are much more likely to go undetected when data is fragmentary and technology solutions for investigators are geared towards compliance-style checks on individual entities. Moreover, the use of analytics allows FIs to analyse financial crime risk at scale and permits much more proactive identification of risk. Accordingly, new technologies are likely to increase the value and usefulness of the information exchanged. The below case study provides examples on the benefits achieved in a 2018-2020 data sharing proof of concept in the United Kingdom.

Box 4.1. United Kingdom Tribank Pilot

The TriBank Pilot, which took place in the United Kingdom in 2019, involved three large banks combining pseudonymised transactional data (i.e., dates, amount, and tokenised sender and receiver accounts) in order to be analysed holistically. Personally Identifiable Information (e.g., names and addresses) were not disclosed by participant banks. The Pilot demonstrated that pseudonymised transactional data can be collected from multiple participant FIs safely and effectively, can be combined and linked into a meaningful unified dataset, and analysed centrally. The technology platform demonstrated that without any knowledge of the underlying transacting accounts, large and complex clusters can be identified automatically, singled out among the broad account base, and brought forward as candidates for further analysis by the participating institutions.

This pilot demonstrated two complementary approaches to collaborative AML/CFT analytics: 1) the participating FIs provided initial information about suspicious/concerning accounts, and the platform significantly expanding this leading intelligence to show the "big picture"; and 2) the platform itself automatically identified significant areas of concern without any leading intelligence being provided by the FIs. The two approaches work symbiotically to create an effective cross-bank transaction monitoring framework, which enables each participating institution to contribute its own intelligence and to benefit from the other institution' intelligence without anyone having to disclose any confidential customer information.

28. Some respondents also noted that in some regions, with the emergence of FinTech s and other new market participants to the banking sector, customers are moving away from traditional incumbent banks and using multiple institutions for banking, instead of banking with a single FI with a large market share. This means data about individual customers is becoming increasingly dispersed across a wide array of FIs, thereby making it more difficult to gain ML and TF insights based on the data available to a single institution alone. This creates a further incentive for private-to-

private data sharing and collaboration in order to bring together sufficient data sets to apply advanced analytics to more accurately assess customer risks or identify potential suspicious activity.

29. Nevertheless, data processing must be proportionate in relation to the legitimate purpose pursued. At all stages of processing, a fair balance between all interests concerned and rights must be assured. Precisely, personal data must be processed fairly and in a transparent manner and collected for explicit, specified and legitimate purposes, in compliance with data retention rules. All facets of data sharing and the use of technologies – including AML/CFT effectiveness and the DPP and competition impacts – should first be assessed so that all aspects are appropriately taken into account before projects are deployed.

4.2. What are the stated goals for private-to-private data pooling initiatives?

30. While not an exhaustive list, FIs may decide to share data, including outside financial groups and potentially across jurisdictions, to facilitate:

- The employment of customer due diligence ***measures***, such as:
  - *Institutional Risk Assessment:* to more accurately gauge ML/TF risks to employ better metrics for new products and services.
  - *On-boarding customers*: to identify if a natural or legal person has previously raised flags or concerns with another institution within or outside of a financial group; verifying the risk rating of customers by checking the existence of similar behaviour across business lines.
  - *Transaction monitoring*: to detect layering by examining the transaction pattern of a customer to assess the financial profile; to follow-up on any abnormal activity detected across institutions; to better identify suspicious activity; to apply transaction thresholds.
  - *Risk management of a business relationship*: to update customer information on an ongoing basis; identify global risk exposure as a result of on-boarding of the same customer across multiple institutions; and dynamic risk management to reflect new information or changes in customer behaviour.
  - *Identification of the beneficial owner*: to enhance the accuracy on the identification of beneficial owners; to identify the same beneficial owner across institutions; to enhance the detection of shell companies; or to develop a more efficient record-keeping of beneficial owner information.
- The end-to-end ***technical-flow***, such as:
  - *Identification of typologies of crime*: to more rapidly and accurately identify emerging criminal typologies and implement safeguards, as well as share findings with other institutions and the public sector.
  - *Intelligence driven investigations*: to align investigative efforts and reach more definitive investigative conclusions.

31. Based on the results of the Questionnaire, the primary reason to share or pool data for AML/CFT purposes is for transaction monitoring. However, some respondents noted that the purpose of such initiatives could include multiple options from the aforementioned list. The below chart summarises the responses to the

Questionnaire, which identify the various purposes for FIs to share AML/CFT information.

Figure 2. Primary Purpose for FIs to Share AML/CFT Information

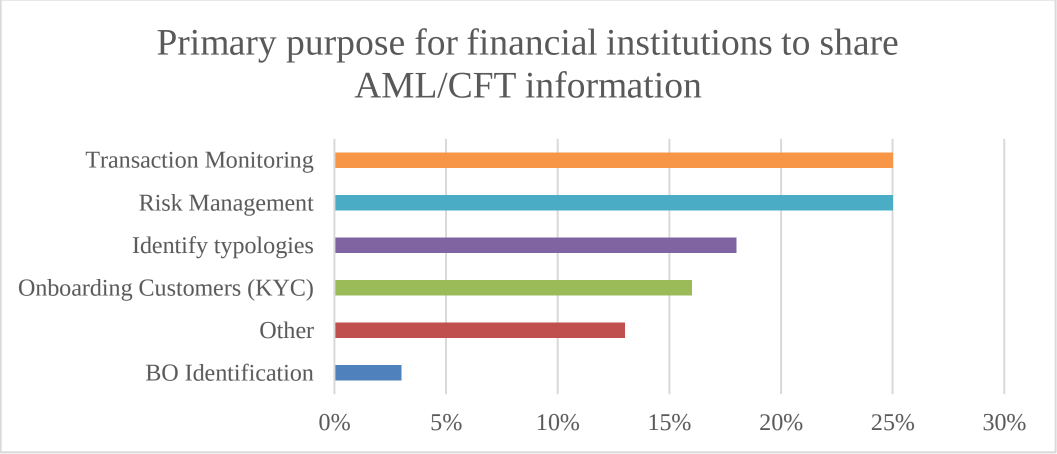


Table Note: Each respondent could only select one answer from the above list.

32. Examples of "other" reasons for sharing of AML/CFT data include:

- risk reduction to facilitate better decision-making in detecting, preventing, and investigating AML/CFT, more generally;
- to facilitate feedback loops for developing and optimising data processing parameters;
- to conduct intelligence driven investigations; and
- to facilitate the development of data driven criminal typologies.

4.3. What type of data could be shared?

33. To achieve the aforementioned specific objectives, encrypted shared data could include: CDD information; transactions; red flags; indications of customer risk, such as whether a STR has been filed; and updated information of the institutions in a correspondent banking relationship, including customer information where it can facilitate risk assessments and ongoing due diligence by the institutions.

34. According to the results of the Questionnaire, the primary *type* of data shared (presently or under consideration) is customer information (which includes beneficial ownership information), information related to red flags and transaction data. Respondents noted that a combination of data categories is often shared, depending on the specific objective of the initiative. However, some respondents also noted that the sharing of customer information is only occurring in an encrypted state and in the context of a limited proof of concept. The below chart summarises the results of the Questionnaire, to identify the main types of information presently shared, or under consideration by respondents to the Questionnaire.

Figure 3. Primary Types of Information Shared

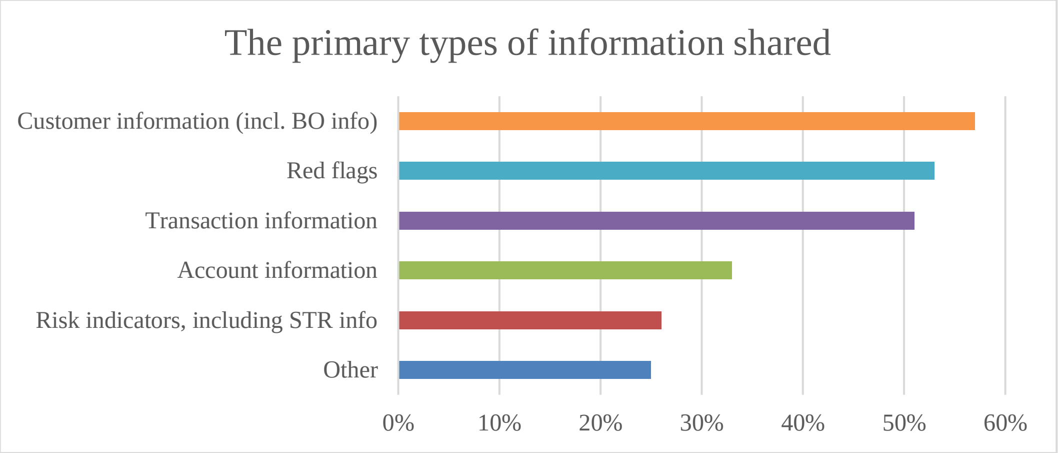


Table Note: Each respondent could select up to all answers from the above list.

35. Examples of “other” types of data shared include:

- legal entity identifier (LEI)[11] reference data;
- typologies; and
- alert dispositioning/outcomes (for internal model tuning).

[11] The Legal Entity Identifier (LEI) is a 20-digit, alpha-numeric code that enables clear and unique identification of legal entities participating in financial transactions. For more information, see “Introducing the Legal Entity Identifier (LEI)”, Global Legal Entity Identifier Foundation (GLEIF), www.gleif.org/en/.

Box 4.2. Japan's Proof of Concept on Machine Learning and Artificial Intelligence

In order to facilitate data sharing consistent with DPP regulations, Japan has developed a unique proof of concept (POC) project, which includes participation from several Japanese FIs, supported by the Japan Financial Services Agency and sponsored by the New Energy and Industrial Technology Development Organisation. This project integrates AI algorithms with instructions from each FI transaction dataset, without sharing or pooling the data, resulting in a single AI model.

This POC aims to build an AI model to facilitate human judgement by calculating the likelihood of a true positive score for transaction monitoring and sanctions screening.

In this POC, the transaction data of individual FIs were not shared or pooled, but rather took the following two approaches: (1) integrating the AI models themselves that learned each institutions' dataset; and (2) tuning the AI model that had already learned the dataset of one institution to re-learns another bank and continued this process to improve the accuracy of this AI model.

According to the results of this project, the Shared Transaction Monitoring and Screening System with AI has enough potential to reduce workload, including the triage process of the detections and dealing with false positives. In terms of accuracy and interpretability, the results indicate that some human operations at the conventional triage process can be replaced by AI-powered judgement. If this initiative spreads to a wider range of financial industry participants, it could improve the efficiency and effectiveness of AML/CFT as a whole.

4.4. Drivers and preconditions for the use of new technologies

36. This section summarises the present landscape of the use of new technologies for private-to-private data sharing and collaborative analytics for AML/CFT purposes, as well as identified enabling environments, drivers and preconditions that contribute to the development and subsequent deployment of such technologies.

37. According to the Questionnaire results, only 40% of respondents stated that FIs in their jurisdiction are using new technologies to share or pool data with other FIs for AML/CFT purposes. Of those respondents, 72% stated that such initiatives were jointly developed by the public and private sectors.

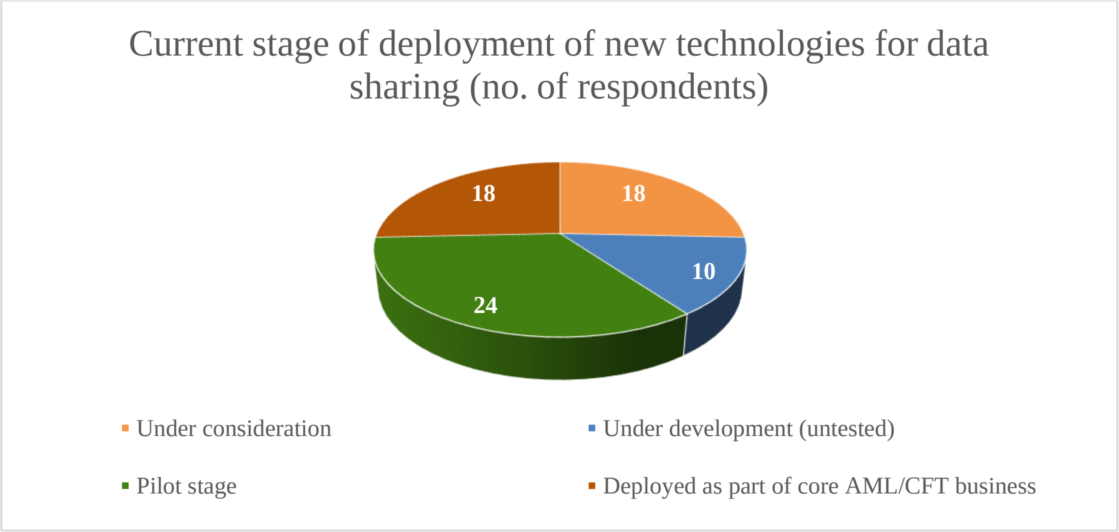
38. The below case study provides an example of a co-developed model for a private-to-private AML/CFT information sharing arrangement.

Box 4.3. China's Information-Sharing Platform Trial

Under the guidance and supervision of the People's Bank of China - AML bureau, there is a trial operation of an AML risk information sharing platform (henceforth, "information-sharing platform") amongst several Chinese FIs that integrates blockchain, digital identity, and trusted privacy-enhancing technologies. This trial platform allows participating FIs to encrypt high-risk customer information, including digital identity number (DID) and risk labels identified by the institution and then upload it to the blockchain. When a participating institution inquires about the customer, a match is made on the block chain through a secure computing platform. DID will only be matched when and if that searched individual's name and national ID number have been uploaded by other participating FIs. After matching, the sharing platform extracts the ML risk information and returns it in cipher text to be decrypted; the processing unit also immediately deletes any records of such computations. Then the inquiring FI will be alerted that an individual is also high-risk at another FI or be inquired by other FIs. Therefore, in this project design, there is no actual exchange of customer data amongst institutions.

39. The responses to the Questionnaire also reveal that the majority of initiatives that use new technologies to facilitate private-to-private collaborative analytics and data pooling are currently in the nascent stages of development and testing. For instance, the majority of respondents (74%) noted that the stage of deployment for such technologies was either still under consideration or in the development/testing phases. The below chart outlines the responses to the Questionnaire on the current stages of deployment of these new technologies.

Figure 4. Stage of Deployment of New Technologies for Data Sharing



40. As illustrated in the below table, respondents noted that the various initiatives to test and use new technologies for data pooling and collaborative analytics are driven by the private sector, particularly large multinational FIs, retail and commercial banks and internet based firms (FinTech and other).

Figure 5. Drivers of the Development and Implementation of New Technologies

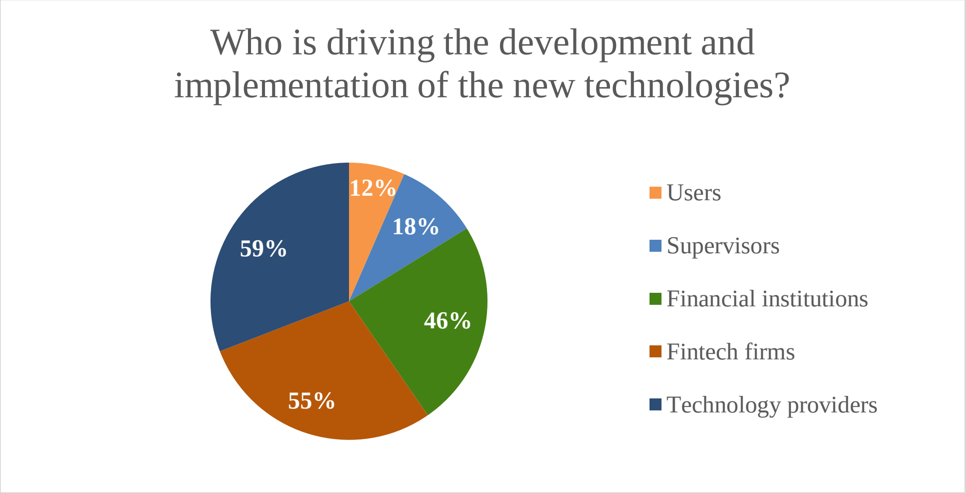


Table Note: Each respondent could select multiple answers from the above list.

41. Other drivers for the use of new data sharing technologies included the emergence of technological developments that promise to improve AML/CFT effectiveness and efficiency, and having in place favourable and clear regulatory frameworks to deploy new technologies for private-to-private data sharing.

42. In some jurisdictions, AML/CFT regulators and supervisors have engaged closely with the private sector to encourage the development of new approaches and technologies for AML/CFT collaborative analytics and data pooling. Some respondents noted, in particular, that AML/CFT supervisors and DPP authorities are consulted when developing new projects. Open dialogue with supervisors and authorities was noted by the private sector as essential to the success of initiatives using new technologies and their ultimate effective implementation.

43. In some cases, legislative amendments were noted as a prerequisite to the deployment of private-to-private collaborative analytics technologies. In such cases, engagement with AML/CFT policy makers and AML/CFT supervisors is therefore a necessity to the success of these initiatives. The below case study outlines a private sector-led initiative to pool AML/CFT data, which requires legislative amendments for its future deployment. This case study demonstrates the importance of open dialogue between various competent authorities and private sector participants.

Box 4.4. Transaction Monitoring Netherlands (TMNL)

TMNL is a joint initiative of five Dutch banks to collectively monitor their payment transactions to identify signals that could indicate ML or TF. At the time of writing, the TMNL utility is being built.

Through collective transaction monitoring of combined transaction data, the primary goal of this initiative is to improve the detection of money laundering by identifying unusual transaction patterns that individual banks cannot identify alone. As such, TMNL will focus on so-called multi-bank alerts. In addition to this collective monitoring platform, participating banks will continue to monitor their own transactions in accordance with their existing obligations under Dutch AML legislation.

The transaction data to be pooled by participating Dutch banks will only relate to transactions executed on bank accounts administrated in the Netherlands. In the longer term it is foreseen that other banks can join TMNL as well. Once in operation, if TMNL flags a potential unusual transaction or series of transfers indicative of presumed ML or other illegal activities, all participants of the payment chain will receive an alert relating to the transaction(s). The receiving banks will independently review the alerts from TMNL and individually decide whether to file an unusual transaction report to the Dutch FIU (the decision whether or not to report will not be shared in the platform). Currently, at the time of writing, this project is focusing on transaction information related to corporate clients.

TMNL is presently building the platform required to receive all the transaction data, to combine them for collective transaction monitoring and to report presumed unusual multi-bank alerts to the participating banks. The platform will be Cloud-based and is being built on a copy of a so-called accelerator platform of one of the participating banks. One of the design principles of the tailor made platform will be the componentised set up, which will allow for use of state-of-the art tools going forward. The privacy sensitive information of the transaction data to be exchanged between the banks and TMNL will be pseudonymised.

In order to develop this project, Dutch participating banks have been working closely with government partners, such as Data Protection Authority, the Ministries of Finance and Justice and Security, the Fiscal Information and Investigation Service and the FIU. The formation of TMNL aligns with the 2019 ML Action Plan announced by the Dutch Government. As part of this plan, an amendment of the AML/ATF Act is foreseen to enable full-scale collective transaction monitoring.[12] The amendment seeks to enable Dutch banks to share more transaction data and information on presumed unusual transactions, to lift the ban on outsourcing of their transaction-monitoring processes, and allow for the use of the Civil Service Number, the unique private individual identification number, in the collective transaction monitoring process.

44. In addition to open dialogues between FIs and AML/CFT and DPP national authorities, respondents noted the value of regulatory sandboxes (or innovation hubs) to test how new technologies interact with national (or supranational) AML/CFT and DPP laws and regulations. However, as outlined in a recent report by the FinTech Working Group of the United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA), regulatory sandboxes can be complex to set up and costly to run.[13]

45. Questionnaire respondents noted that sandboxes and innovation offices/hubs were highlighted as both drivers and enabling environments as they facilitate and encourage the development and implementation of new approaches, by assisting participants in the identification of opportunities, risks, vulnerabilities, and mitigation measures. The below box includes examples of a regulatory sandbox and innovation hub for new technologies to share AML/CFT data.

[12] At the time of writing, the legislation to permit the activities of TMNL is currently still being developed and as of yet has not been brought before parliament.

[13] UNSGSA FinTech Working Group and CCAF. (2019). Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech. Office of the UNSGSA and CCAF: New York, NY and Cambridge, UK.

Box 4.5. Enabling Regulatory Environments

United Kingdom

The Financial Conduct Authority (FCA) held a TechSprint in 2019 which examined how encryption techniques known as privacy enhancing technologies can facilitate the sharing of information about ML and financial crime concerns, while remaining compliant with data security laws. This event included representatives from industry to showcase their initiatives, technology and results achieved, and included attendance from AML supervisors and representatives from the UK Information Commissioners Office (ICO). The FCA recently ran a Digital Sandbox Pilot to provide certain support, including access to synthetic banking transaction data sets, to innovative firms looking to develop new solutions and products to combat fraud and scams. Several of these firms are employing PET technologies in the development of these solutions. The pilot concluded in February 2021 and will inform future iterations of a digital testing environment.

France

The French Autorité de Contrôle Prudentiel et de Résolution (ACPR) has created a FinTech innovation hub to connect the innovative financial ecosystem. This dedicated small team, open to all innovative project holders, plays the role of an innovation observatory. It is also responsible for the "suptech" mission – i.e. integrating new technologies in supervisory tasks - within ACPR. The ACPR FinTech innovation hub has led four working groups in the past two years related to AML-CFT. Gathering industry representatives and public authorities (FIU, security and data protection authorities), these working groups addressed issues such as distant KYC, AML-CFT processes in the crypto-asset sectors, relationships between banks and crypto-asset services providers with an AML perspective, etc. In addition, the ACPR FinTech innovation hub has engaged a dialogue with academics on the opportunities and regulatory challenges of new technologies in the financial sector. In this context, in March 2020, the ACPR organised an event around data sharing and data pooling that highlighted how cutting-edges techniques enable sharing the knowledge without necessarily sharing the data. For instance, privacy guarantees provided by differential privacy can be used to train predictive models – for example those embedded in transaction monitoring systems – on data too sensitive to be disclosed to any given financial institution. Yet another technique is secure multi-party computation, a building block for secured collaborative processes such as producing KPIs on fraudulent IBANs based on transactions and user data pooled from multiple FIs.

46. Finally, respondents also highlighted the need to conduct thorough data protection impact assessments when developing new technologies for data pooling and collaborative analytics. In some countries, such assessments are a regulatory requirement prior to data processing to minimise identified risks to the rights of individuals.

5. New Technologies Identified to Share and Analyse AML/CFT Information

47. This section summarises the various new technologies currently under development or in use to facilitate data sharing and analysis between FIs for AML/CFT purposes. These new technologies were identified in the course of desk-based research, and interviews with respondents.

5.1. Identified technologies for private-to-private information sharing

48. The below table summarises the various new technologies under consideration to facilitate private-to-private collaborative analytics and data pooling. The most cited technology used for data pooling and collaboration was cryptography, and for the analysis of large data sets was machine learning. However, respondents to the Questionnaire often noted that data sharing and analysis initiatives require the use of multiple types of technologies in order to secure and analyse large data sets, and to ensure it is in line with national and international DPP requirements. Therefore, the various technologies outlined in the below table are often applied together to ensure data security and protection.

Table 5.1. Summary of technologies for private-to-private AML/CFT collaborative analytics

Type of technology	Description	Examples of potential benefits for AML/CFT data sharing
Cryptography/Encryption Technologies		
Homomorphic encryption	It allows organisations to cross-match and search third-party data assets without identifying the contents of the search or compromising the security or ownership of the underlying data. This means different parties can collaborate on sensitive data while preserving privacy, confidentiality, and regulatory compliance. (Microsoft, 2016[2])	To enable access to a wider set of data to improve outcomes and enable intelligence-led decision making by reducing false positives, advancing the efficiency of financial crime investigations, improving enterprise data quality, and enabling greater operational efficiency.
Zero-knowledge proofs	In essence, a zero-knowledge proofs is a cryptographic method and verification method that takes place between a prover and a verifier. The prover is able to prove to the verifier that they have information without disclosing the underlying data or information itself.	The technology would allow Bank A to establish whether Bank B held data on an individual, without sharing that individual's identity.
Secure-multiparty computation (SMPC)	SMPC enables several parties to evaluate a function on private data coming from distinct data sources without aggregating or sharing the data. At the end of the protocol, the parties learn nothing more but the value of the function. (Scheibner, 2020[1])	This technology may be applied to disparate data sources to extract credible suspicions from different parties, while keeping the data sovereign.

Type of technology	Description	Examples of potential benefits for AML/CFT data sharing
Differential Privacy	Involves cryptographic protocols that permit each party to maintain the anonymity of its own data while working with different parties to carry out joint computations on their collective inputs.	This technology may create a trade-off between precision of data and privacy, which might imply that it would be best suited for analysing broad trends rather than detecting anomalies or detailed patterns.
Advanced Analytics		
Machine Learning (supervised, unsupervised and reinforced learning)	Is a sub-field of AI where computers are able to learn (via learning algorithms) when exposed to new data, instead of being explicitly programmed to perform certain tasks.	Supervised learning methods can be used to develop compliance risk scoring models based on historical examination/audit results. Decision points in business processes can be optimised by machine learning models by understanding the current states and predicting optimal decisions. A scoring model or a classification mode can be used for identifying suspicious networks or entities from financial transactions or other relevant data.
Federated Learning	Federated learning is a machine learning technique that trains an algorithm across multiple decentralised databases that contain local data. The algorithm learns new information (e.g. trends) in each disconnected database without exchanging or moving the data. (Shiffman, 2020[2])	For example, a travelling algorithm can access and interrogate data sets in different FIs without moving the data. The purpose is for the algorithm to learn new types of criminal trends and techniques that it would not be able to learn if it resided in only one institution. This leads to more dynamic risk assessment tools, such as dynamic red flag indicators.
Deep Learning	Deep Learning is a field of machine learning that uses multiple layers of learning algorithms to extract meaning from large quantities of data.	For example, can be deployed by FIs for transaction monitoring.
Natural language processing	Natural language processing helps computers communicate with humans in their own language and scales other language-related tasks. For example, NLP makes it possible for computers to read text, hear speech, interpret it, measure sentiment and determine which parts are important. (SAS, 2020[3])	For example, can be deployed to transform free text in STRs into structured data that can be used for network analytics. Using text mining, STRs or any documents, can be annotated automatically to facilitate better retrieval later on.
Robotic process automation	Software automation technology where “robots” (i.e. a software program) are programmed based on human behaviour in order to mimic such interactions to carry out numerous repetitive tasks, at high volume and with speed and accuracy.	Enhances efficiency by automating repetitive tasks that were previously performed by humans.
Network Analytics	Network analytics is the use of network data to detect potentially obscured trends and patterns in large pools of data. It allows visualising intricate networks of entities and attributes of the identified linkages.	To derive patterns that cannot otherwise be seen at end-point level. Network analytics can be used to identify network of related entities based on known subject(s) of interest.
Infrastructures for Processing and Transfer		

Type of technology	Description	Examples of potential benefits for AML/CFT data sharing
Trusted execution environments (confidential computing)	Confidential computing is the protection of data-in-use through isolating computations to a hardware-based trusted execution environment. This environment is protected by securing a portion of the hardware's processor and memory. (Microsoft Azure, n.d.[4])	For example, two parties agree to share their data (e.g., transaction data) and analyse it using a trusted execution environment.
Secure cloud technology	Cloud computing is the delivery of information technology services over the internet that allow businesses and governments to accelerate innovation and collaboration Cloud security involves the procedures and technology that secure cloud computing environments against both external and insider cybersecurity threats. (McAfee, 2020[5])	Advances in cloud technology have enabled firms to collect, store, and analyse significantly large data sets at very low costs. This technology allows for the storage and analysis of both structure and unstructured data, and can be used to facilitate collaboration amongst those with access to the secure cloud environment. However, regardless whether two FIs have their data in the same cloud environment, the legal barriers for data sharing remain the same.
Distributed Ledger Technology	It is an encrypted, common ledger of transactions maintained by parties in a network. With no single central authority controlling the ledger, it is an extremely secure and transparent way to store information in an, on principle, immutable and chronological record. (OECD, n.d.[6])	For example, can be used as a way to share data between several parties, without one party having the full power of data disposal. However, the legal barriers for data sharing remain.
Application programming interfaces (API)	An API is an interface that allows regulated institutions to submit data. It facilitates communication between regulated institutions and authorities by integrating data production process, allowing for greater automation and lower reporting costs. (FSB, 2020[7])	Allows large data sets to be collected, stored and analysed more efficiently.

49. The below case studies offer examples on new technologies in use or in development to facilitate collaborative analytics for AML/CFT by FIs (see Annex B for additional Regtech case studies).

Box 5.1. Federated Learning

A team of hardware technology provider and software vendors are working on launching a secure, federated learning platform where machine learning models can be trained across multiple data sets to detect and analyse "normal" and "abnormal" patterns. In these platforms, the model moves across the databases in different locations and the data never moves. This allows the model to learn new criminal trends and techniques based on the participating institutions' data sets while preserving privacy and security. The knowledge gained within the model can then be used to continuously refine and tune risk indicators across participating institutions.

Box 5.2. Secure Multiparty Computation

A Regtech has developed technology that enables two or more FIs to collaboratively compute a risk assessment function, by processing encrypted customer KYC data, as well as behavioural transaction and login activity information without exposing it. This risk assessment function is executed by using privacy enhancing technologies, and does not require entities to actually share or expose customer data in any way or form. The technology uses Multi-Party Computation protocols to process data at each institution without ever exposing the data outside that institution. Participating institutions only exchange completely random strings containing no customer data. The key point is that neither party discloses their data to the other party at any time in a computation. Secure Multiparty Computation obfuscates the computation so that no data appears to be exposed but the result can still be calculated as if the data had been shared in the clear. This technology can be executed before the transaction is actually sent, or in the AML monitoring and analytics phases. The technology also leaves a cryptographic audit trail at each FI. An external auditor provided with the audit trails from all the transacting customers, can reconstruct the whole decision process.

Box 5.3. Homomorphic Encryption

A Regtech has developed a technology-enabled flexible and adaptable trust framework for FIs capable of facilitating secure and private Know Your Customer (KYC) and CDD processes to enhance intelligence-led decision-making. Leveraging homomorphic encryption that uniquely allows data to be processed while remaining encrypted, this initiative enables FIs to securely search, share, and collaborate with third-party data assets without ever revealing the contents of the search itself or compromising the security or ownership of the underlying data. In this decentralised data model, participants are never required to move or consolidate data assets. Data owners maintain control of their data and govern access to it.

In this model, KYC information is validated between multiple trusted participants or jurisdictions without moving or pooling data by allowing the verification of information held by one party against that of another via encrypted search. Analysts were able to securely and privately cross-match and search regulated data across privacy jurisdictions in a business-relevant timeframe while ensuring sensitive assets remained protected during processing in accordance with regulatory requirements. The solution validated how the application of innovative cryptographic techniques can address key challenges in the financial sector, enabling entities to share sensitive information, better understand customer risk, and make faster, better informed decisions to address real-world AML and Financial Crime challenges.

6. Challenges related to the use of new technologies for data collaborative analytics

50. The pooling and collaboration of data amongst FIs, particularly across national borders and with third parties raises a number of policy concerns. While some of these challenges were previously outlined in the aforementioned 2017 FATF Guidance on Private Sector Information Sharing, additional considerations arise when attempting to process larger sets of data while using privacy-enhancing technologies and advanced analytics, such as AI.

51. According to the results of the Questionnaire, DPP requirements were identified as the primary policy consideration when developing and deploying new technologies for private-private data sharing. As outlined in the below chart, other highly cited challenges include regulatory challenges (including explainability/interpretability of new technologies; and a lack of regulatory incentives); and data quality (including a lack of data standardisation).

Figure 6. Main Challenges to Use of New Technologies for AML/CFT Information Sharing amongst FIs

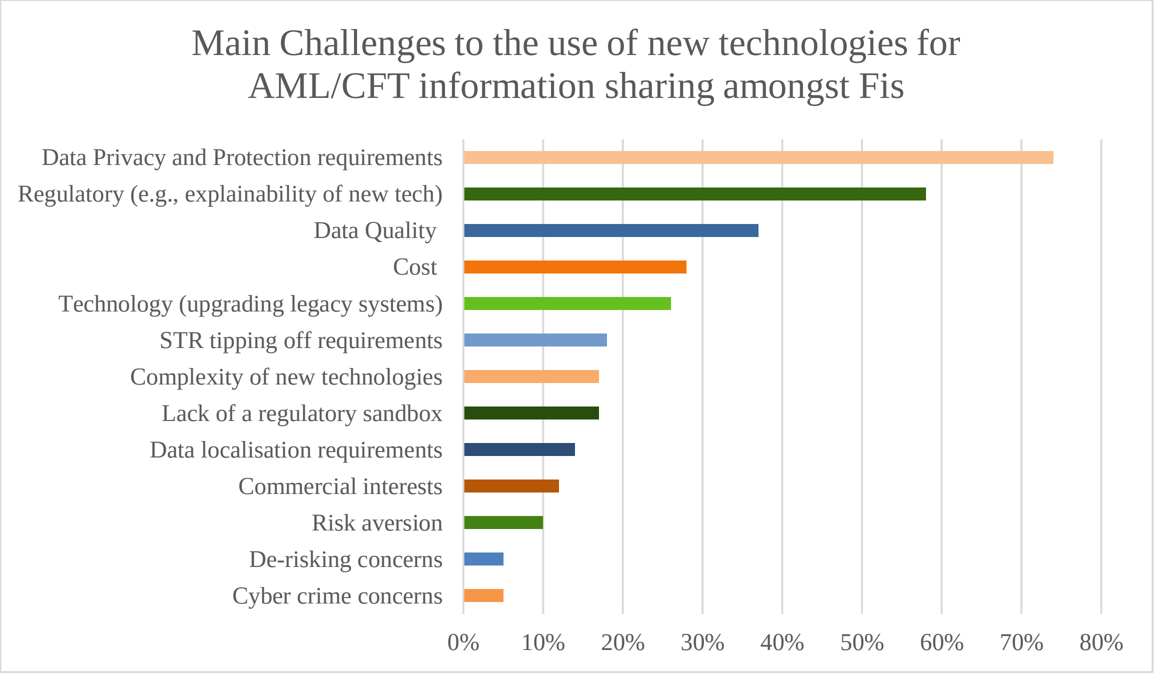


Table Note: Each respondent could select up to four answers from the above list.

52. The following section details the identified challenges and obstacles associated with data pooling and collaborative analytics based on the responses to the Questionnaire, interviews and research.

6.1. Ensuring and Enhancing Data Protection and Privacy

53. AML/CFT and DPP are both significant public interests that serve important objectives, which are neither in opposition nor inherently mutually exclusive.[14] The implementation of data protection principles and rules through international and domestic legal instruments aims to protect human rights and fundamental freedoms, notably the right to privacy. It is essential that legal regimes facilitate both public interests, in order to prevent ML, TF and PF, and other financial crimes, in a way that respects individuals' fundamental rights to privacy and data protection. Financial data may include some of the most sensitive data about individuals, revealing their financial standing, family interactions, behaviours and habits, the state of their health, etc. Therefore, regard must be given to both AML/CFT and DPP and weighed in a balanced fashion, in compliance with Member States' obligations under international law, including human rights law. Under these laws, one of the most crucial requirements is ensuring the existence of a valid legal basis for the processing of personal data. In addition, proportionality in terms of alternative measures to achieve the same goal must be respected. The below case study highlights such requirements in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETs No. 108) opened for signature on 28 January 1981, and was the first legally binding international instrument in the data protection field.

[14] For example, the right to privacy is a universal human right in accordance with the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights, and, at regional level, the European Convention on Human Rights.

Box 6.1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+)

Under Convention 108+, the processing of personal data could be based on: (1) free, specific, informed, unambiguous consent from the data subject for the processing of her/his personal data; or (2) processing (including obtaining) data based on other legitimate basis laid down by law (e.g. performance of a contract, public interest, ensuring public security, legitimate interest of the controller, etc.). Whether the consent, public interest or legitimate interest is required as the valid legal basis, the underlying rationale should be carefully analysed and articulated by international stakeholders from the AML/CFT, DPP and human rights field.

As outlined in Article 11 of Convention 108+, every category of data shared must be clearly defined, as well as the purpose of its processing. This is necessary in order to define for how long it can be retained and if the interference with the right to respect for private life is proportionate and justified. Moreover, Article 6 states that in order to prevent adverse effects for the data subject, processing of sensitive data for legitimate purposes must have additional appropriate safeguards: for instance the subject's explicit consent, a clear legal provision covering this case, a professional secrecy obligation, and a particular technical security measure (such as data encryption).

54. As stated above, ML and TF activities often involve multiple institutions and jurisdictions. In order to better identify suspicious behaviour and mitigate the abuse of the financial system, FIs benefit from sending and receiving information and analysis related to their customers, including across borders. FIs may also want to process larger sets of data to refine their understanding of emerging criminal trends and typologies. Equally, FIs also have a legal obligation to protect their customer's personal data.

55. National, international and divergent DPP laws across jurisdictions may present challenges for FIs when implementing AML/CFT obligations or when developing private sector information sharing initiatives. This issue may be further compounded if there is insufficient regulatory guidance or misaligned approaches towards AML/CFT requirements and DPP obligations. The complexity of different DPP approaches influences the availability, access, processing, and sharing of information by the private sector.

56. A significant challenge to private-to-private data sharing and pooling identified in the course of research and by Questionnaire respondents is the perceived conflict between FIs' desire to share information to improve the efficiency and efficacy of AML/CFT compliance, and existing legal restrictions designed to protect the privacy of its customers. In many jurisdictions, such sharing outside of the financial group context is restricted due to data privacy requirements. Conversely, in one jurisdiction (the United States), exemptions or "safe harbours" exist that allow AML/CFT information sharing between FIs that are not part of the same financial group, as outlined in the box below.

Box 6.2. 314(b) USA PATRIOT Act

Section 314(b) of the USA PATRIOT ACT (Information sharing Between Financial Institutions) provides that two or more FIs and any association of FIs may voluntarily share information with one another regarding individuals, entities, organisations, and countries suspected of possible terrorist or ML activities. A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities that may involve terrorist acts or ML activities shall not be liable to any person under any law or regulation of the US, any constitution, law, or regulation of any State or political subdivision thereof, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure, or any other person identified in the disclosure. (FATF, 2017[8])

To rely on the Section 314(b) safe harbour, it is sufficient that the financial institution or association has a reasonable basis to believe that the information shared relates to activities that may involve money laundering or terrorist activity, and it is sharing the information for an appropriate purpose under Section 314(b) and its implementing regulations. Therefore a financial institution or association can share information relating to activities it suspects may involve money laundering or terrorist activity, even if the financial institution or association cannot identify specific proceeds of an specified unlawful activity being laundered. (FinCEN, 2020[9])

57. The results to the Questionnaire indicate that respondents largely believe that new technologies can address previous concerns related to private sector data sharing, while respecting fundamental and individual DPP rights. A number of respondents also specifically called for national and international rules to clarify when and for what purpose data (and what type of data) can be shared or pooled between FIs for AML/CFT purposes, especially sharing outside of financial groups. In addition, respondents noted the application of new and emerging technologies are not "privacy-preserving" when the aim is to use the data to identify a specific natural or legal person, e.g., on-boarding a customer.

58. While there is a perception that global data protection standards may be needed to foster digital cooperation, no organisation is currently mandated to coordinate their development. Instead, these standards are developed nationally and supra-nationally as governments are responsible for establishing DPP legal frameworks within their jurisdictions. As a result, there is a paucity of guidance as to the kinds of data and information that can be shared between FIs (even with the use of collaborative analytics), and on whether the aforementioned new and emerging technologies and processes enable organisations to remain compliant with national and supranational privacy requirements.

59. According to the United Nations Conference on Trade and Development, 132 out of 194 countries have enacted some form of legislation to secure the protection of data and privacy. (UNCTAD, 2020[10]) That said, the level of safeguards and DPP

compliance varies considerably among States. The entry into force of the EU GDPR, has not only harmonised DPP rules within the EU and European Economic Area, but it has also acted as a catalyst for many countries around the world to consider modernising privacy rules.

60. The below case study presents the EU's data protection rules.

Box 6.3. EU's Data Protection Rules

The rights to privacy and to data protection are enshrined in the EU Charter of Fundamental Rights (Articles 7 and 8).

The EU GDPR, which entered into effect on 25 May 2018, regulates how companies process personal data of individuals. The GDPR, *inter alia*, requires companies to only collect and process personal data that is necessary (i.e., data minimisation) to fulfil a specific and defined purpose (i.e., purpose limitation) and not further process in a manner incompatible with those purposes. It also requires that individuals are informed amongst others, on when their data is collected and the purpose(s) for which the data will be processed. It sets a limitative list of legal basis allowing to process personal data and establishes a set of individual rights, including the rights of access, rectification and erasure, as well as the right not to be subject to decisions solely based on automated processing, including profiling.

The GDPR is supervised and enforced by the data protection authorities (DPAs) in each EU Member State. The EDPB, which is made up of representatives from each DPA and the European Data Protection Supervisor, ensures that GDPR is applied consistently throughout the EU.

Transfers of personal data to third countries or international organisations are subject to very specific conditions so as to ensure that guarantees of the GDPR are not undermined. This transfer can, in particular, be based on "adequacy decisions" adopted by the European Commission when the level of data protection in a third country is essentially equivalent to the one guaranteed in the EU.

Importantly, the GDPR notes that data protection principles do not apply to anonymised data (namely personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable), which falls outside of the scope of its requirements. Pseudonymised data (i.e., personal data that can no longer be attributed to a specific data subject without the use of additional information), on the other hand, is considered personal data and falls within the scope of the GDPR.

61. While DPP laws may differ between each jurisdiction, there is a trend towards convergence. For instance, there is a trend towards adopting data protection frameworks sharing similar key features [i.e., an overarching law rather than sectoral rules, a core set of data protection principles and obligations, the empowerment of individuals with enforceable rights to control their data (e.g., data rectification and erasure), and, the creation of an independent supervisory

authority with enforcement powers]. Moreover, international standards such as the Convention 108+ – the only multilateral legally binding instrument on data protection – the OECD Privacy Guidelines and others point to a positive trend in that context. The United Nations is also developing recommended legislative provisions and a compendium of existing good practices on data protection rules to facilitate international cooperation in counter-terrorism ("UN CT Programme on Data Protection").

62. But, as noted in the 2017 FATF Guidance on Private Sector Information Sharing, it can be challenging or impossible for FIs to rely upon consents or public interest exemptions to process customer data for the purposes of combatting financial crime, including by transferring them to other parties. In addition, the conditions for legality for international transfers must be met. Express legal provisions providing for appropriate safeguards or guidance defining the circumstances in which, where possible, customer data can be transferred across jurisdictions for such purposes can help facilitate information sharing. (FATF, 2017[8])

63. Nevertheless, even where there is a valid legal framework in place to authorise private sector data transfers, the data shared by a FI may be inaccurate or incomplete. Therefore, although data pooling and collaborative analytics could support other FIs for AML/CFT compliance (e.g., performing CDD), the FIs using this data remain responsible for ensuring its accuracy. FIs should therefore verify the quality of shared data, by assessing whether the elements collected and the checks carried out by other FIs are up-to-date, suitable and sufficient for the fulfilment of their AML obligations.

64. In some jurisdictions, FIs, as data controllers, are required to provide individuals with access (on request) to the information they collect, transmit and retain.[15] The intent is to allow individuals to understand what data is available on them so that they can request to correct or delete inaccurate and unnecessary information (i.e., right to rectify or erase such data under certain conditions). Tension may arise if individuals suspected of illegal activities or under formal investigation request the deletion of incriminating information. However, legislation may provide for certain (and duly justified) restrictions when the exercise of individual rights may affect the compliance with a legal obligation or when an ongoing investigation risks being jeopardised.

65. Another challenge exists for those jurisdictions that permit transfers of personal data that is anonymised. Some respondents to the Questionnaire noted that there is ambiguity in relation to the ability of organisations to share anonymised data as there is a perception that the requirements for anonymisation[16] and pseudonymisation[17] lack clarity or may vary across jurisdictions.

66. Furthermore, rules on international transfers may affect private-to-private data sharing (outside of financial groups). In many cases, public authorities or private

[15] For example, see Article 9 Convention 108+.

[16] Anonymous data describes information not related to an identifiable natural person, or information where the data subject is no longer identifiable (and there is no possibility for re-identification). (ICO, What is Personal Data? Accessed December 2020, <ico.org.uk>.

[17] Pseudonymisation is a security measure that replaces or removes information in a data set that identifies an individual. However, this data is still considered a personal data as the data subject could be re-identified (e.g., if someone holds an encryption key). (Ibid.).

entities are unable to transfer data out of their jurisdiction without equivalent protections in the target jurisdiction or appropriate safeguards to ensure data protection. In addition, data localisation laws may typically involve two main requirements: (1) that personal data about citizens are hosted in data centres located in a country or group of countries; and (2) that data is manipulated and processed inside the same country. This also places restrictions on the transfer of information based on the legal framework of each jurisdiction. As a result, FIs may be prohibited from sharing specific data with counterpart FIs on suspicions of financial crime risk across national borders, as well as within the same financial group, or may not be shielded from liability for doing so as in a domestic context.[18]

67. Finally, respondents to the Questionnaire noted that an impediment to the wider deployment of new technologies for data pooling and collaborative analytics is the lack of interaction between national and international AML/CFT and DPP authorities. Such lack of coordination and cooperation might implicate FATF's Recommendation 2 requirement for cooperation and, where appropriate, coordination between relevant AML/CFT authorities to ensure the compatibility of AML/CFT requirements with DPP rules.

6.2. Data Quality

68. Data standards and formats vary significantly across institutions, jurisdictions, infrastructures and message networks. These differences can impede the use of data analytics, delay banking processes, and increase the cost of compliance. Low quality data, including inaccurate or out-of-date data, could also nullify the benefits of data pooling and collaborative analytics as it could result in an erroneous analytical outcome. Automated and advanced analytical tools, in particular, depend on standardised inputs.

69. Based on the Questionnaire results, data quality represents a major challenge to the deployment of advanced analytics in in centralised or decentralised data sets. Respondents specifically noted that the data quality of some FIs is poor, and there is variation and incompatibility of data standards across FIs. Data quality remains a major obstacle to produce the data sets needed – in the correct and consistent format – to prevent biased conclusions, which could, in a worst case scenario, lead to financial exclusion. These challenges are amplified when data is overlaid with an encryption layer as this makes it more difficult to identify errors in the data, which can in turn lead to errors in output.

6.3. Lack of Regulatory Clarity

70. A significant number of Questionnaire respondents noted that the lack of explicit regulatory requirements and guidance for the use of new technology is a challenge for private sector data pooling and the use of collaborative analytics. Some jurisdictions are seeking to clarify or adapt their rules in order to allow data sharing and collaborative analytics between FIs, and a few jurisdictions have financial intelligence sharing partnerships in place. Some respondents noted that in the absence of guidance and certainty from the regulator, there is less of an incentive to

[18] For further information, see (IIF, 2019[17])

prioritise the investment and implementation of expensive new technologies that could facilitate collaborative analytics.

71. One respondent also noted that the current legal frameworks were not created with the possibilities of using new privacy enhancing technologies in mind, and therefore do not clearly describe the boundaries for the applications of such techniques.

72. Finally, a number of respondents also noted that existing national regulations bar private-to-private data sharing completely (except if the exchange of information occurs within financial groups).

6.4. Explainability and Interpretability

73. In January 2020, the European Banking Authority (EBA) released a paper on the use of big data and advanced analytics in the European banking system. This paper notes that European FIs appear to be at an early stage of using advanced analytics that uses simple machine learning models and prioritises explainability and interpretability. One of the challenges associated with employing more complex analytical models is their explainability and interpretability to regulators, as well as the potential for bias and unintended results. According to the EBA, a model is explainable when its internal behaviour can be directly understood by humans (interpretability) or when explanations (justifications) can be provided for the main factors that led to its output. (EBA, 2020[11]) In the absence of such understanding, the technology can be perceived as a 'black box' by regulators. This could affect its deployment, as regulators are unable to conduct adequate inspections, risk assessments, and appropriately manage and mitigate any identified risks associated with the use of such technology. This is especially the case when a decision is based on a high level of automation and has a direct impact on customers. To address such challenges, regulators could work with public and private sector technologists and other relevant stakeholders to evaluate and help drive adoption of appropriate practices to explain, document, and govern advanced analytics in the context of AML/CFT applications.[19] This work could include whether and how explainability requirements could be applied pursuant to a risk-based approach—e.g., imposing more stringent explainability requirements as the potential impact of the model on business continuity and/or potential harm to customers increases.

74. Some Questionnaire respondents noted that FIs have been deterred by implementing new AML/CFT technologies for data sharing and analysis as regulators expect cryptography and machine learning models that can be clearly understood. This is particularly challenging if the technology has been developed by a third party vendor who has proprietary rights over the technical specifications underlying the technology, or for those FIs who lack human resources with adequate technical literacy on advanced cryptography and analytics. One respondent also noted that in the regulators' view, algorithmic models should be

[19] See U.S. federal banking agencies' Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence. See also a similar initiative by FinReglabs and Stanford University, following a request for information by U.S. federal banking agencies, that seeks to evaluate emerging practices to explain, document, and govern machine learning models for lending underwriting: https://finreglab.org/ai-machine-learning/explainability-and-fairness-of-machine-learning-in-credit-underwriting/

designed in a way that allows for results to be reproduced given the same input data, which is not always possible with machine learning.

75. An important element raised by Questionnaire respondents is the need for manual (human) intervention to review the outcome of advanced analytics (e.g., AI and machine learning) to ensure the accuracy of the results and to continuously refine the algorithmic models. Hybrid approaches – where humans review more complex analytical outcomes as they are freed up from performing basic routine tasks that can be completed by simple models – were noted by respondents as a good practice. However, respondents also noted concerns that some advanced analytics may be used by an FI without an in-depth understanding of the functioning and objective of the technology and may result in unverified and unreliable outputs. Similarly, AML/CFT supervisors should also understand or have access to a team who can understand the advanced analytical models to test how FIs have designed and validated their models.

76. Finally, respondents noted that it is important that regulated entities can confirm not only to their supervisor but also to themselves that any new technology being deployed is producing better outcomes than the previous system, especially in areas where it can be unclear whether the technology is improving AML/CTF effectiveness.

6.5. STR Confidentiality and Tipping Off

77. STR confidentiality rules can impede the ability to share STRs (or the fact that a STR has been filed or the underlying STR information). STR confidentiality is critical to the effective functioning of the reporting regime. Confidentiality of STRs is essential so that the subject of STR and third parties are not tipped-off, as this can adversely affect intelligence gathering and investigation, and can enable persons to abscond with or dispose of assets. Confidentiality also protects the reputation of the person who is the subject of an STR. Finally, confidentiality protects the safety and security of the person filing the report, and breaches of confidentiality have the potential to undermine the entire STR regime. Unauthorised disclosure of STRs could also result in a FI facing criminal liability in many jurisdictions. These concerns place necessary limits on the sharing of STRs. (FATF, 2017[8])

78. STR confidentiality is even more complex when the sharing occurs across national borders, where different national laws exist. These may include, for example, national provisions relating to discoverability and production of available records in judicial proceedings. While some countries have regulations that require regulator notification of judicial requests and subpoenas concerning domestic STRs so that the regulators can intervene to ensure STR confidentiality in the legal proceedings, these regulations may not protect foreign STRs submitted to a foreign FIU.

79. While STR confidentiality can create challenges for private-to-private information sharing, it is important to prevent tipping-off. Alternative legal or technological mechanisms that guarantee the anonymisation or encryption of personal data may be able to provide safeguards without a corresponding cost to AML/CFT effectiveness.

6.6. Market Structure and Competition

80. Widespread collection and analysis of data is not a new phenomenon, however, technological innovations now allow the ability to store significant amounts of data and analyse it instantaneously. The larger the amount of data, for example, the more likely it is that the analytical outcome will be more accurate. Currently, only large incumbent FIs have sufficiently vast data sets to use advanced data analytics efficiently. Therefore, there is a need to raise awareness on cross-institution processing of data in order to ensure that small to mid-sized FIs may also benefit from these new technologies. This will also ensure that any cost advantages associated with the use of such technology could be shared.

81. As noted by a number of Questionnaire respondents, the processing of large sets of customer information between FIs could potentially raise competition concerns. This could result in selective sharing of data with only a small group of "trusted" participants, resulting in an uneven sharing framework. Therefore, there might be a transfer of ML/TF risks from FIs that have information sharing mechanisms to those lacking such arrangements. Bad actors that are thwarted by the former group may then gravitate towards the latter group to reduce the possibility of detection. FIs or sectors that lack information sharing mechanisms may thus face additional ML/TF risks, and additional risk mitigation may have to be considered.

82. FIs may also be reluctant to share commercially sensitive information that has the potential to distort competition in the market. Varying IT capabilities of FIs may also hinder the effective sharing of information, as differing or inadequate IT systems and diverse data formats are incompatible to pool and run collaborative analytics across. Similarly, this may disadvantage institutions that rely on legacy IT infrastructure and systems, and therefore result in their exclusion from data sharing initiatives.

83. Access and exchange of data amongst a limited number of FIs should not provide them with an unfair advantage as competitiveness of financial services firms is increasingly shaped by access to real time big data sets. Therefore, competition law concerns may also have a place in the assessment of an AML/CFT data sharing arrangement, by ensuring that a level playing field is maintained and exclusionary conduct by potential competitors avoided. Hence, when data access is warranted it must be granted on fair, reasonable and non-discriminatory terms and in a manner that does not enable or facilitate collusion. Furthermore, the data exchange must be limited to what is strictly necessary.

6.7. Technology Costs and Constraints

84. A number of Questionnaire respondents noted that the scalability of privacy enhancing technologies and advanced analytics, in particular, is impacted by the significant start-up cost of such technology. While large FIs may have the resources to invest in such technology or purchase licenses to access third party technology, many small or middle-sized institutions are still lagging to update existing legacy technologies. This may also result in a reduced pool of data, as it may only include data from institutions that can afford the start-up costs associated with such technology.

85. Advanced analytics, such as machine learning, were also noted by Questionnaire respondents as expensive to implement and maintain. This is further compounded

by the need to integrate new analytics with legacy systems, leading to additional upgrade costs. The trialling of new advanced analytics while simultaneously running existing systems was also noted as barrier due to the excessive costs involved. Moreover, an additional cost associated with the use of advanced analytics is the need to maintain technical human experts who have sufficient expertise of the technology in order to develop complex models and to refine them over time.

86. An additional technological challenge of pooling and analysing large amounts of data is the need to have sufficient computing power in place to run the algorithmic models. The size of data sets can significantly influence the cost of computing.

87. The pooling or sharing of AML/CFT data could also involve, for example, the transfer of a large data set including information on transactions and customers. Such large data sets are "heavy" and difficult to move (i.e., referred to as data gravity). It is therefore essential to consider data gravity when developing data pooling initiatives, and the growth potential of the data gravity once centralised.

88. Finally, an additional challenge to deploying advanced analytics, such as machine learning, in the context of AML/CFT is the need to validate data, or confirm whether an individual pattern was truly indicative of criminal conduct. Model validation can be particularly difficult in the context of ML/TF, where investigations may take several years before concluding. In many cases, FIs are not informed of the ultimate outcome of the STR filed to the FIU, and whether the reported activities led to a ML or TF conviction.

6.8. Defensive Reporting and De-risking

89. A commonly stated use for collaborative analytics for AML/CFT purposes is to identify criminal conduct across multiple FIs. By leveraging privacy enhancing technologies, for instance, an institution may be able to overcome data localisation and STR confidentiality requirements and gain insight into whether an STR was filed against their customer by another institution, but without obtaining the sensitive underlying data. However, this has the possibility of exacerbating defensive STR filing behaviour. Overreliance on a system of sharing suspicious information could potentially lead to a situation where an FI would regard a customer as suspicious based solely on third party information, which may be inaccurate or the grounds for suspicion was ultimately rejected by the financial intelligence unit. This could have the unintended and unethical impact of denying a legitimate customer's access to the financial system, or subjecting customers to further clarifications on the nature and purpose of their transactions, resulting in delays in the execution of the bank's services.

90. Moreover, the mere existence of a suspicion does not necessitate the systematic filing of an STR by other institutions that receive such information. Instead, it may be an important element for an institution's analysis of risk and result in enhanced CDD measures. Therefore, the introduction of widespread collaborative analytics and data pooling may result in increased instances of identified suspicions (particularly where defensive reporting has occurred), and could result in a substantial increase in the application of enhanced CDD measures, which could lead to an increase in the cost of compliance. This could discourage the use of this technology or lead to de-risking behaviour.

6.9. Security

91. The introduction of new technology to pool and process data also introduces new and significant vulnerabilities and possibilities for cybercriminals to identify and exploit security vulnerabilities. For example, the use of technologies to establish a centralised data pool raises serious cyber security vulnerabilities, as well as national security concerns. It also raises important policy considerations about who is ultimately responsible for monitoring the security of these data repositories, and who would be accountable for failures or cyber-attacks. Pooling larger quantities of data would also create the possibility of a catastrophically large data leak by a single party. Accordingly, insider threat protections are more important as data pooling and sharing possibilities grow.

92. Advancements in collaborative analytics using pseudonymisation technologies offer some protections, provided that identifying information is kept separately and is subject to technical and organisational measures to ensure that personal data is not attributed to an identified or identifiable natural person. Nevertheless, despite the advancements in pseudonymisation technologies, data protection legislation still applies and the risk of re-identification should also be taken into account, by assessing the time, effort and resources needed in light of the nature of the data, the context of their use, the available re-identification technologies and related costs. Stringent oversight by DPP authorities would also be necessary in initiatives involving collaborative analytics using pseudonymisation technologies.

6.10. Avoidance of Analytical Bias in Artificial Intelligence

93. Concerning the use of data analytics (i.e., AI) for pooled information, a crucial consideration is that any advanced analytics exclude human bias, and therefore prevent discrimination (e.g., based on religion, race, gender, age, sexual orientation, ethnicity, etc.). Bias may be introduced to a system through the introduction (or exclusion) of certain data or in the programming of the algorithmic model.[20] It is imperative that the development and training of these analytics include unbiased data and to develop algorithms that do not reinforce human prejudices or discrimination.

6.11. Human Rights

94. For commercial gains, private sector entities could support the profiling of individuals. This could ultimately lead to discrimination, e.g., based on race, gender, political or religious beliefs. Full transparency and a stringent monitoring and/or oversight is therefore needed from supervisory bodies and DPP authorities over any tools implemented for data pooling and collaborative analytics. This includes tools where pseudonymisation techniques are used, as these have the potential of re-tracing to deduce personal data and identities of persons included in the datasets.

[20] For more information on AI ethics, see (FSB, 2017[15]), Annex B.

7. Enabling the wider use of data pooling and advanced analytics

95. According to Questionnaire respondents, the most frequently cited solution to facilitate the greater use of new technologies for data pooling and collaborative analytics, and to address some of the aforementioned challenges, is to promote regulatory certainty around the use of these new technologies. The below section summarises the various solutions that were identified by survey respondents and private sector stakeholders that could contribute to greater use of new technologies for private-to-private data sharing and analysis. These solutions offer a launching point for dialogue between the FATF and the private sector and DPP authorities, and potential future FATF work. These contributing factors to an enabling environment for the wider use of data pooling and collaborative analytics are not presently endorsed by the FATF.

7.1. Regulatory Clarity

96. Questionnaire respondents noted that there is an increasing urgency to develop a data framework encompassing all the areas surrounding sharing or pooling of data by the private sector, including for AML/CFT data. Questionnaire respondents replied that this could be achieved through enhanced collaboration between AML/CFT authorities (including regulators) and DPP authorities. This may help foster a proper enabling environment that could mitigate risk aversion from the industry due to the current perceived lack of clarity. A large proportion of respondents also called for clear guidance from national financial regulators as to the kinds of data that can be shared between FIs, and on whether certain technologies (e.g., homomorphic encryption, etc.) and processes enable organisations to remain compliant with national and supranational privacy requirements, in addition to the financial-sector-specific regulations. This could provide organisations with the assurances needed to proceed with investments in technology, training, human resources, and production deployments of data sharing solutions. Similarly, some respondents called for the consolidation and publication of strong use cases of new technologies (i.e., best practices), detailing how certain new technologies may address privacy concerns in relation to private-to-private data sharing.

97. Some respondents also called for national legal safe-harbour provisions, which permit voluntary data sharing between FIs for defined AML/CFT purposes based on principles of necessity and proportionality.

98. In regard to STR tipping-off requirements, some respondents have called for changes to the regulatory STR requirements, enabling FIs to more freely share information as to whether an STR has been filed against a particular person, or the underlying STR data.

7.2. Promotion of Enabling Environments

99. A number of respondents also called for AML/CFT supervisors to launch more pilot programs, regulatory sandboxes and innovation hubs to allow new technologies for data sharing and analysis to be tested without punitive or overly aggressive regulatory enforcement as the FIs undertake implementation phases. Such initiatives would foster innovation in this area as FIs would not be subject to

supervisory criticism even if the pilot ultimately proves unsuccessful. The success of such initiatives is also impacted by the level of engagement and involvement of national DPP authorities. Such engagement could facilitate alignment, common learning, and increased clarity on issues such as model governance, modelling techniques and how data analytics can target particular ML/TF risk areas and facilitate data sharing, while respecting DPP requirements.

100. The FATF has also identified *Suggested Actions to Support the Use of Technology in AML/CFT* (see Annex C) that advance the 2017 San Jose Principle to *pursue positive and responsible innovation*. These Actions note that new technologies for AML/CFT must be developed and implemented in a way that reflects threats as well as opportunities, ensuring that their use is compatible with international standards of data protection and privacy, and cybersecurity.

7.3. Data Standardisation and Governance

101. In order to enhance data quality, some respondents called for the standardisation of formats for data collection, as well as to promote the use of open APIs to enable customers to share data between FIs. Jurisdictions could then use their compliance powers as a feedback mechanism to inform FIs of the data quality requirements and enforce appropriate measures to improve the quality to acceptable levels.

102. In relation to data governance, respondents stressed the need for FIs to put in place data governance policies, frameworks and controls to ensure:

a. the quality of data, including completeness of data, how recently data was collected or updated, whether the data is structured in a machine-understandable form, and whether the source of the data would affect the interpretation of or reliance on the data. This also would include means of assessing the veracity of data; and

b. the origin of data is tracked, including keeping an audit trail of data.

103. The use of digital identities for identification was also referenced as a possible solution to address data quality as it could become a standard tool to support the third party reliance on identification, thereby contributing to increased data sharing. Similarly, LEIs could be used as a documentation source for the CDD of legal persons. The inclusion of the LEI could ensure that a unique identifier is associated with each legal person, instead of reliance on name matching.

104. Finally, in interviews with respondents the Common Reporting Standard (CRS) was referenced as a model. The CRS calls on jurisdictions to obtain specific information from their FIs and automatically exchange that information with other jurisdictions on an annual basis to counter tax evasion. (OECD, n.d.[12])These respondents believe that this model could inform the discussion on data quality for information sharing for AML/CFT purposes, as it includes specific data standardisation requirements (i.e., specifying the information to be collected and exchanged).

7.4. Bias Prevention in Artificial Intelligence

105. Finally, in relation to the prevention of human bias and discrimination in AI, respondents stressed the importance of regularly reviewing the legitimacy and credibility of data sources, extensive model validation, and continuous model monitoring. For example, data sets, which may be under or over representative of

certain groups of people may need additional training data to improve accuracy and fairness.

106. In addition, the OECD's Principles on AI, adopted in May 2019 by OECD member countries, state that AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society. AI systems must also function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed. It is therefore imperative that the ethics of using predictive models in a regulatory context are fully understood at the outset as those organisations and individuals developing, deploying or operating AI systems could be held accountable for their proper functioning. (OECD, 2019[13])

8. Concluding Remarks

107. The outlined considerations surrounding private-to-private sector AML/CFT data sharing are not new to the FATF. However, available and emerging technological advancements may offer new ways to share and analyse data in order to more efficiently and effectively detect potential suspicious activity or comply with other AML/CFT obligations. New technology may also offer solutions to better protect personal data, with the goal to ensuring that any exchange or processing of information respects national and international DPP legal frameworks. Nevertheless, the compliance of the considered developments with the data protection requirements of a jurisdiction needs to be duly assessed before implementation in order not to impede the protection of fundamental rights. In some jurisdictions, for example, such initiatives may not presently be legally permissible.

108. This Stocktake identified available or emerging technologies that facilitate data pooling and collaborative analytics between FIs, and examined the policy considerations, legal challenges and potential solutions raised by respondents. This report acknowledges that data pooling and collaborative analytics initiatives present a number of important policy considerations. For instance, it is important that data pooling and collaboration initiatives equally weigh and mitigate any risks related to de-risking and the denial of a legitimate customer's access to the financial system prior to their execution. The FATF will build upon this Stocktake paper by continuing this dialogue between AML/CFT supervisors, technology developers, FIs, and DPP authorities, and other relevant experts to ensure that new technologies that can contribute to enhanced AML/CFT effectiveness may be fully utilised, consistent with DPP national and international frameworks.

Annex A. Glossary

- **Advanced Analytics**: Advanced analytics refers to the autonomous or semi-autonomous examination of data or content, using sophisticated techniques and digital tools, typically beyond those of traditional business intelligence, to discover deeper insights, make predictions, or generate recommendations. Advanced analytic techniques include those such as data/text mining, machine learning, pattern matching, forecasting, visualisation, semantic analysis, sentiment analysis, network and cluster analysis, multivariate statistics, graph analysis, simulation, complex event processing, neural networks. Advanced analytics typically rely on the use of big data.
- **Application:** An application is computer software designed to help a user perform specific tasks.
- **Application Programming Interface (API):** An API is a set of definitions and protocols for building and integrating application software. APIs let digital products or services readily communicate with other products and services.
- **Algorithm:** A computer algorithm is a set of step-by-step instructions to perform a specific task.
- **Artificial intelligence (AI)**: An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments (and operate with varying levels of autonomy). (OECD, 2020[14]) The goal of AI is to enable computers to automate some aspects of analysis—potentially saving human labour for more subtle tasks and gaining insights humans might not reach. There are several component technologies within AI all with numerous applications. There is no consensus as to what constitutes "thinking" and "intelligence" or what is "fully autonomous," and there are several categories of AI, but in general, to varying degrees, AI systems build "smart machines" that combine intentionality, intelligence, and adaptability. At present, machine learning is the most familiar and developed form of AI.
- **Big data:** The Financial Stability Board defines big data as "the massive volume of data that is generated by the increasing use of digital tools and information systems," such as financial transaction data, social media data, and machine data (e.g., Internet of Things, computer and mobile phone data. (FSB, 2017[15])
- **Black Box**: Black box refers to AI/machine learning and other technologies that are opaque, non-intuitive and do not provide adequate information regarding their decision-making and predictions/results –i.e., black box technology lacks explainability.
- **Benchmarking**: Benchmarking is an approach to determining the actual and relative capabilities of a technology-based process, product or service and identifying performance gaps by testing it against the best performance being achieved for the function, task, or goal—whether within the particular entity or organisation, industry-wide, or achieved by a different industry—using hard performance data measured by specified benchmarking criteria.

Benchmarking may be used to measure [compare] the performance of new technology vs legacy systems, or one new technology against alternative new technologies.

- **Collaborative Analytics:** For collaborative analytics, data is not moved to a central location in order to analyse them together with other data assets. Instead, the analytical tools come to the data, not the other way around. This makes it easier to keep the data secure and to ensure control over who accesses what data for what purposes.
- **Cybersecurity:** Cybersecurity, a broader term than data security, refers to the comprehensive process of protecting data and the systems for moving, storing, and authenticating that data.
- **Data pool/pooling**: Data pooling refers to a process where digital data from different sources are combined, resulting in a fuller and more useful data set for analysis (including by multiple parties). These pools are organised in a centralised manner.
- **Data security:** Data security refers to the process of protecting data from unauthorised access and data corruption throughout its lifecycle. It includes data encryption, hashing, tokenisation, and key management practices that protect data across all applications and platforms. Data security is narrower than cybersecurity.
- **Data standardisation**: Data standardisation is the process of converting data to a uniform format to enable users to process and analyse it. Data standardisation is essential to enable big data processing and advanced analytics, and the development and application of other innovative digital tools and methodologies. For example, financial data can vary within and across entities; data standardisation converts it into a common form that enables sophisticated large-scale analytics.
- **Digital Identity (ID) Systems/solutions:** Digital ID systems/solutions are identity systems or products and services that carry out the process of identifying/verifying a (natural or legal) person's identity, binding the proofed identity to a digital credential, and using the digital credential(s) and potentially other authentication factors to establish (confirm) that a person claiming the identity is the identity proofed person (i.e., is who the person claims to be).
- **Distributed Ledger Technology (DLT) (a.k.a. blockchain):** DLT refers to a type of technology protocol that enables simultaneous access, validation, and updating of an immutable ledger (digital record) distributed across multiple computers (and typically, across multiple entities or locations)—i.e., DLT creates a distributed digital database.
- **Deep Learning (DL):** DL is an advanced type of machine learning in which artificial neural networks (algorithms inspired by the human brain) with numerous (deep) layers learn from large amounts of data in highly autonomous ways. DL algorithms perform a task repeatedly, each time tweaking it a little to improve the outcome, enabling machines to solve complex problems without human intervention.

- **Digitalisation:** Digitalisation is the use of digital technologies and digitised data to change a business model, impact how work gets done, transform how customers and companies interact, and provide new revenue and value-producing opportunities.

- **Digitisation:** Digitisation is the conversion of data, information, text, pictures, sound or other representations in analogue form into a digital form (i.e., binary code) that can be processed by computer.

- **Dynamic data:** Dynamic data refers to a continuous real-time digital stream of data points that are known to be in constant flux, so that the data set constantly changes over time, as distinct from static or persistent data that is mostly unaffected by time.

- **Explainability**: In the context of new technologies, explainability means that technology-based processes, solutions, or systems are capable of being explained (explicated), understood, and accounted for. Explainability provides adequate understanding of how solutions work and produce their results. Explainability is a basic condition for trust and responsible use. Explainable AI technology provides transparency into the data, variables and decision points used to achieve a result.

- **FinTech:** FinTech refers broadly to the use of new and emerging digital technologies in the financial sector for any of a wide variety of purposes. Initially, "FinTech" primarily referred to the application of technology-based innovations to provide new customer-facing financial products and services [e.g., mobile payment solutions, online marketplace lending, algorithmic savings and investment tools, virtual currency payments, capital raising (crowd funding) and deposit taking (remote check capture, mobile banking)]. FinTech now also encompasses the use of new and emerging technologies to provide automated mid- and back-office enterprise functions, such as the use of algorithms, big data, AI and machine learning, and link analytics for wholesale clearance, settlement, and other wholesale intermediation for e.g., securities, derivatives, wholesale finance, and payments, as well as regulatory compliance activities (see RegTech definition, below). Other applications remain to be developed

- **Fuzzy logic:** Fuzzy logic is a subset of AI that takes an open, imprecise spectrum of data (imprecise input) and processes multiple values in a way that produces output that includes a range of intermediate possibilities between YES and NO (e.g., certainly yes, possibly yes, cannot say, possibly no, certainly no). Fuzzy Logic systems produce definite output in response to incomplete, ambiguous, distorted, or inaccurate (fuzzy) input, simulating human decision making more closely than conventional yes/no logic. Fuzzy logic can be implemented in hardware, software, or a combination of both.

- **Internet of Things (IoT):** The global network of all Internet-enabled devices and machines that are connected to the Internet and can collect, send, share and act on data, using embedded sensors, processors and communication hardware, without human interaction. The IoT generates an enormous amount of real-time data that can be analysed and used to create desired actions or business outcomes (see big data).

- **Interoperability**: refers to the ability of different information technology systems and software applications to communicate, exchange data, and use the information seamlessly in real-time, enabling all participants operate across all systems.

- **Machine Learning:** Machine learning is a type (subset) of AI that "trains" computer systems to learn from data, identify patterns and make decisions with minimal human intervention. Machine learning involves designing a sequence of actions to solve a problem automatically through experience and evolving pattern recognition algorithms with limited or no human intervention—i.e., it is a method of data analysis that automates analytical model building.

- **Machine Readable Regulation:** Machine readable regulation replaces rules written in natural legal language with computer code to enable the use of artificial intelligence for regulatory reporting purposes.

- **Natural language processing (NLP):** NLP is a branch of AI that enables computers to understand, interpret and manipulate human language. NLP allows humans to talk to machines.

- **Privacy Enhancing Technologies:** "Specialist cryptographical capabilities, which allow computations to take place on underlying data, without the data owner necessarily divulging that underlying data. The same technology can ensure that the data owner does not have visibility over the search query, with the query and the results remaining encrypted (or not disclosed) and only visible to the requester." (Maxwell, 2020[16]) This term therefore encompasses an array of technologies that use encryption and would be useful primarily in allowing the protection of privacy as data is used.

- **Real-time analytics:** Real-time analytics is a machine learning process in which a system processes and analyses data that is loaded instantaneously and almost immediately (in near- real time) generates meaningful output (e.g., information, predictions, or decisions).

- **Real-time data (RTD):** RTD is information that is delivered immediately after collection, ensuring the timeliness of the information provided. RTD enables real-time analytics and can be dynamic or static (e.g. a fresh input indicating a specific location at a specific time).

- **Regulatory Technology (RegTech):** RegTech is a sub-set of FinTech that uses new technologies to comply with regulatory requirements more efficiently and effectively than existing capabilities

- **Responsible Innovation:** Innovation is responsible when it is fit for purpose and complies with applicable regulatory requirements, including AML/CFT, consumer protection, cybersecurity, and privacy protections.

- **Smart machines:** Computer hardware and software systems that use AI algorithms. Smart machines are designed to make decisions, often using real-time data. Unlike passive machines that are capable only of mechanical or predetermined responses, smart machines use sensors, digital data, and remote inputs, combine information from these different sources, analyse this input instantly, and act on the insights derived from the data. Smart machines mimic human intelligence by using advanced computational process to reach conclusions based on their instant analysis.

- **Static data:** Static data refers to a fixed data set—data that remains the same after it is collected.
- **Supervised learning**: Supervised learning is a machine learning process that teaches algorithms predictive models by feeding the algorithm input data with known outcomes—i.e., supervised learning teaches algorithms by example. The input/output pair (labelled data) provides feedback for the algorithm, which uses the training data set to adjust the model to minimise error. For example, a training set may contain pictures of different kinds of animals with a label associated to each picture, allowing the algorithm to compare the predicted label with the correct one. Supervised learning uses a validation data set to measure the algorithm's progress in learning the model and a test data set to evaluate the model's performance on never-before-seen data to determine whether the model has learned its training data effectively and can generalise to new data.
- **Supervisory technolog**y (**SupTech):** SupTech is the use of innovative technology by supervisory authorities to support supervision and examination.
- **Unsupervised learning (a.k.a. unsupervised machine learning**): Unsupervised learning is a machine learning process that enables algorithms to analyse and cluster *unlabelled* datasets to discover hidden patterns, data groupings or anomalies or anomalies without human intervention. The algorithm parses available data and determines correlations and relationships without an answer key by drawing inferences and grouping like things based on unconstrained observation and intuition. As the amount of data the algorithm is exposed to grows, its modelling becomes more accurate and refined.

Annex B. Additional Regtech Cases Studies on New Technologies for Private-to-Private AML/CFT Data Sharing and Analysis.

Case Study: Encrypted Queries using Homomorphic Encryption Pilot

A Regtech partnered with an FI to implement a privacy enhanced inter-bank information sharing system. The technology, using homomorphic encryption, allows for the deployment of encrypted queries for financial crime and compliance while ensuring regulatory compliance. Currently, the Regtech and FI are working to add additional banks to the pilot, are defining new use cases (including intra-bank cross border use cases around customer risk ratings and model thresholds), and moving towards a production deployment. Homomorphic encryption is specifically used in this initiative to protect sensitive information from being exposed, but still enabling members to use data for analysis and matching between institutions. The advantage of a privacy-preserving analytical capability is that it can enable the distribution of search queries without disclosing the search terms to one another. This negates the risks of disclosure, tipping off, and regulatory breaches, while providing an analytical capability for potential participating institutions. The main obstacle for this project is a lack of regulatory clarity on what type of data can be shared, under what circumstances, and how.

Case Study: German Collaborative Analytical Platform

A FinTech company is partnering with a consortium of top tier banks, software vendors and academics to develop a new collaborative analytical platform for fighting financial crime. The platform will involve a data pool and analytical toolset for transactional and financial data shared between institutions. It will provide fresh insights into criminal behaviour and networks as they manifest across the financial system, not just in individual financial service providers. With this intelligence, financial institutions across Germany and Europe will be able to construct a view of their customer's overall activity network within the broader financial system, thereby tightening the net around money laundering by exposing hidden relationships and patterns of transactional behaviour previously masked from view.

Case Study: Nordic KYC Platform

A Regtech company was founded in 2019 by six of the leading banks in the Nordic countries as a joint initiative to address challenges in AML regulations for the Nordic market. The six founding banks developed a common data standard for KYC-information, which is made available through the company's KYC services and digital platform including an end-customer/user portal. The company's platform is fully independent and accessible to participating financial institutions requiring effective and compliant KYC-information. This ensures that financial institutions can access and use this KYC information as foundation for their own risk assessments. It also benefits their customers since financial relationships becomes easier with a more customer friendly experience. Control over the customer relationship stays with the institution. The Company ensures privacy of personal data across the solution by applying a secure hybrid cloud architecture based on privacy and secure by design principles.

Case Study: Financial Crime Index

Bank A started using the Regtech Financial Crime Index to strengthen their approach to financial crime risk. The Index leverages a bank's own data combined with publicly available sources and the Regtech's proprietary dataset to generate a monthly overall financial crime risk score, in addition to scores and reports across nine financial crime risk themes.

Case Study: Secure end-to-end Encryption Platform

A Regtech has built an information and data-exchange platform that enables banks and other FIs to exchange AML-relevant information. The information exchanged through the platform can be used for one-to-one messaging (requests for information / RFI's) or one-to-many "data pooling", helping FIs to: (1) resolve both more basic inquires (e.g. sanction alerts that need extra information from the counterparts' FI), (2) more complex joint investigations (e.g. investigating 2nd level transaction monitoring alerts that involve multiple institutions) and (3) enriching data used for the high risk customers due diligence process (e.g. sharing info about PEP's RCA's, UBO's, source of funds, etc.).

The platform is built using end-to-end encryption. All data exchanged is protected by encryption keys and backed by password protection. One-sided encryption and hashing is used for data pooling, so FIs can share information with multiple parties, with hashing verifying the data or files exchanged are authentic. The platform host does not have access to any unencrypted data and the platform ensures full auditability by logging all critical activities.

Case Study: Blind Matching of Records using Homomorphic Encryption

A software company worked with a public authority on a pilot that enabled blind matching of records using homomorphic encryption. The public authority wanted to gather and link data from a range of private and public sources, including multiple FIs, for statistical purposes to inform public policy. The solution provider used a combination of technical and structural controls to allow data contributors to submit encrypted data to the recipient such that:

1. Only encrypted data left contributor environments.
2. Data could not be linked prior to it reaching the recipient. The recipient required a third-party (an intermediary) to convert the encrypted contributor data to a linkable, tokenised dataset.
3. The recipient was not able to reverse the processing and obtain original, raw contributor data, but was able to link the datasets.

The pilot successfully demonstrated that the solution enabled the linking of data on a common attribute without that attribute being visible to any party after leaving the recipient environment. This protects the privacy of the individuals while still allowing for population analysis to inform policy making. The technology is now in production in the UK, being used by National Health Service Digital.

Annex C. Suggested Actions to Support the Use of Technology in AML/CFT

A responsible use of new technologies, including digital identity and cutting-edge transaction monitoring and analysis solutions (including collaborative analytics) can assist effective, risk-based implementation of the FATF Standards by the public and private sectors, as well as promote financial inclusion.

The following principles advance the San Jose Principle to *pursue positive and responsible innovation* endorsed by FATF in 2017. New technologies for AML/CFT must be developed and implemented in a way that reflects threats as well as opportunities, ensuring that their use is compatible with international standards of data protection and privacy, and cybersecurity.

1. Create an enabling environment by both government and the private sector for responsible innovation to enhance AML/CFT effectiveness:

i. *Innovative solutions that facilitate the implementation of AML/CFT measures, including risk assessments, CDD and other requirements, and strengthen their supervision and examination.*

ii. *Good practices for updating internal legacy systems or replacing them with new technologies.*

iii. *Appropriate safeguards and features for new AML/CFT solutions, including: explainability and transparency of processes and outcomes; oversight by humans; respect for privacy and data protection; strong cybersecurity; and alignment with global, national, and technical standards and best practises.*

2. Ensure Privacy and Data Protection when implementing new technologies:

i. *Ensure there is a valid legal basis for the processing of personal data when deploying new technologies.*

ii. *Protect personal information in line with national and international legal frameworks.*

iii. *Process data for an explicit, specified and legitimate purposes, consistent with national and international rules.*

iv. *Support the responsible development and adoption of innovative privacy-preserving technologies to enable robust AML/CFT information sharing and analysis, while preserving privacy.*

3. Promote AML/CFT innovation which supports financial inclusion by design

i. *Mitigate the obstacles to financial inclusion through the development and implementation of innovative solutions*

ii. *Ensure responsible innovation consistent with the FATF objective to promote financial inclusion*

4. Develop and communicate policies and regulatory approaches to innovation that are flexible, technology-neutral, outcomes-based and in line with the risk-based approach

i. *Consider the impact of new technologies holistically, in the context of the structural and organisational changes that accompany them, their possible unintended consequences, and their overall impact on AML/CFT effectiveness, and financial inclusion.*

ii. *Issue and/or update clear policy statements, guidance, use cases, best practises or regulations, as necessary to inform and encourage the responsible use of new technologies for AML/CFT*

iii. *Consult with counterparts and regulated entities to inform relevant policy and decision-making processes.*

5. Exercise informed oversight

i. *Build expertise in new technologies, to enable informed regulation and supervision of their use, including for specific AML/CFT compliance purposes.*

ii. *Identify explicit, well-defined uses of new technologies for AML/CFT supervision and examination*

iii. *Understand the risks and benefits associated with new technologies, and appropriate risk-mitigation measures that preserve their benefits.*

iv. *Use technology to enhance AML/CFT supervision*

6. Promote and Facilitate Cooperation

i. *Co-operate and co-ordinate with all relevant authorities to facilitate a comprehensive, coordinated approach to understanding and addressing risks and benefits in the use of new technologies for AML/CFT, including data protection and privacy authorities.*

ii. *Consider developing collaborative environments to facilitate cross-government and/or public private research and development of new technologies and innovative solutions.*

iii. *Participate in international efforts to develop global principles governing the use of new technologies for AML/CFT to help ensure their alignment with human rights, the improvement of the implementation of global AML/CFT, cybersecurity, data privacy and protection measures, as well as relevant technical standards and trust frameworks.*

References

EBA (2020), *Big Data and Advanced Analytics*. [13]

EDPB (2020,), *Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf. [1]

FATF (2017), *Guidance on Private Sector Information Sharing*, https://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-information-sharing.html. [10]

FinCEN (2020), *Section 314(b) Fact Sheet*, http://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf. [11]

FSB (2020), *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions*, p. 32, http://www.fsb.org/2020/10/the-use-of-supervisory-and-regulatory-technology-by-authorities-and-regulated-institutions-market-developments-and-financial-stability-implications/. [9]

FSB (2017), *Artificial intelligence and machine learning in financial services*, https://www.fsb.org/wp-content/uploads/P011117.pdf. [17]

GLEIF (n.d.), *Introducing the Legal Entity Identifier (LEI)*, http://www.gleif.org/en/. [21]

IIF (2019), *Data Flows Across Borders – Overcoming Data Localisation Restrictions*, http://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf . [19]

Maxwell, N. (2020), *Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime*, http://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf. [18]

McAfee (2020), *What is Cloud Security?*, http://www.mcafee.com/enterprise/en-us/security-awareness/cloud.html. [7]

Microsoft (2016), *Homomorphic Encryption*, http://www.microsoft.com/en-us/research/project/homomorphic-encryption. [2]

Microsoft Azure (n.d.), *Confidential computing*, https://azure.microsoft.com/en-us/solutions/confidential-compute. (accessed on December 2020). [6]

OECD (2020), *AI Principles*, https://www.oecd.ai/ai-principles. [16]

OECD (2019), *Principles on Artificial Intelligence*, http://www.oecd.org/going-digital/ai/principles/. [15]

OECD (n.d.), *Blockchain Primer*, http://www.oecd.org/finance/OECD-Blockchain-Primer.pdf (accessed on December 2020). [8]

OECD (n.d.), *What is the CRS?*, http://www.oecd.org/tax/automatic-exchange/common-reporting-standard/ (accessed on December 2020). [14]

SAS (2020), *Natural Language Processing*, http://www.sas.com/en_us/insights/analytics/what-is-natural-language-processing-nlp.html. [5]

Scheibner, J. (2020), *Data protection and ethics requirements for multisite research with health data: a comparative examination of legislative governance frameworks and the role of data protection technologies*, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC7381977/pdf/lsaa010.pdf. [3]

Shiffman, G. (2020), "Federated Learning through Revolutionary Technology (White Paper)". [4]

Tim Hulsen, T. (2020), *Sharing is Caring—Data Sharing Initiatives in Healthcare*, http://www.mdpi.com/1660-4601/17/9/3046/pdf. [20]

UNCTAD (2020), *Data Protection and Privacy Legislation Worldwide*, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. [12]

STOCKTAKE ON DATA POOLING, COLLABORATIVE ANALYTICS AND DATA PROTECTION

Technological advances in recent years have made it possible for financial institutions to analyse large amounts of data more efficiently and to identify patterns and trends more effectively. Data pooling and collaborative analytics can help financial institutions collaborate to better understand, assess and mitigate money laundering and terrorist financing risks. The FATF has examined innovative technologies that will make it easier and more effective to identify criminal activity, while reducing false positives and preventing criminals from exploiting information gaps between financial institutions.

The report also highlights the need to protect data protection and privacy: AML/CFT and data privacy and protection are both significant public interests that serve important objectives. New and emerging privacy-enhancing technologies offer promising ways to protect information in specific use cases and in line with national and international data protection and privacy frameworks.

www.fatf-gafi.org | JULY 2021