FATF

PARTNERING IN THE FIGHT AGAINST FINANCIAL CRIME

DATA PROTECTION, TECHNOLOGY AND PRIVATE SECTOR INFORMATION SHARING

JULY 2022

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 (2022), *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*, FATF, Paris, France, https://www.fatf-gafi.org/publications/digitaltransformation/documents/partnering-in-the-fight-against-financial-crime.html

Photocredits coverphoto: Gettyimages

Table of Contents

Acronyms

AML	Anti-money laundering
CDD	Customer due diligence
CFT	counter-terrorist financing
CoE	Council of Europe
CPF	counter-proliferation financing
DPA	Data protection authority
DPIA	Data protection impact assessment
DPP	Data protection and privacy
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FI	Financial institution
FinCEN	U.S. Financial Crimes Enforcement Network
FIU	Financial intelligence unit
GDPR	General Data Protection Regulation
HRIA	Human rights impact assessment
IAS	incident alert system
ICCPR	Covenant on Civil and Political Rights
ICO	Information Commissioner's Office
KYC	Know your customer
MAS	Monetary Authority of Singapore
ML	Money laundering
NPO	Non-profit organisation
OECD	Organisation for Economic Co-operation and Development
PET	Privacy enhancing technology
PF	Financing of proliferation of weapons of mass destruction
SAR	Suspicious activity report
STR	Suspicious transaction report
TF	Terrorist financing
UN	United Nations
UTR	Unusual transaction report

Executive Summary

Countering money laundering (ML), terrorist financing (TF), and the financing of proliferation of weapons of mass destruction (PF) and data protection and privacy (DPP) are significant public interests. Both serve important objectives, including upholding human rights and fundamental freedoms[1] (such as the right to privacy) and protecting the public from criminal activities, including terrorism. These interests are not in opposition nor inherently mutually exclusive. An effective regime for anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/CFT/CPF) requires the public and private sector to pursue both AML/CFT/CPF and DPP objectives.

This report aims to help jurisdictions that are considering enhancing information exchange among private sector entities to design and implement such initiatives responsibly, in accordance with data protection and privacy rules, so that the risks associated with increased sharing of personal data are appropriately taken into account. To strike an adequate balance, the FATF has consulted data protection authorities, academics, technology providers and the private sector in this work.[2]

AML/CFT/CPF systems seek to deprive organised criminal groups, corrupt officials, terrorist organisations, weapons proliferators, or drug or human traffickers from accessing the financial system. Despite these efforts, criminal organisations are becoming more sophisticated and taking advantage of gaps in the system. A single financial institution has only a partial view of transactions and sees one small piece of what is often a large, complex puzzle. Criminals exploit this information gap by using multiple financial institutions within or across jurisdictions to layer their illicit financial flows. Without more accurate and consistent information, it becomes increasingly difficult for individual financial institutions to detect these activities. By using collaborative analytics, bringing data together, or developing other sharing initiatives in responsible ways, financial institutions seek to build a clearer picture of the puzzle, to better understand, assess, and mitigate money laundering and terrorist financing risks.

Importantly, the collection and use of personal data for these purposes can trigger data protection and privacy concerns. Misuse of data, unnecessary sharing, or a lack of protections have the potential to negatively impact individuals who are not engaged in malicious activities. Relevant data and systems must be managed and designed in accordance with applicable DPP rules. Where the legal framework requires, it is important that the initiatives are necessary, reasonable and proportionate in relation to the purposes of processing (i.e., AML/CFT/CPF). Initiatives need to be designed and implemented responsibly and effectively so that the risks associated with increased sharing of personal data are appropriately taken into account. In general, these risks need to be outweighed by the public benefits of combating financial crime.

In this report, members of the FATF and its Global Network share experiences of increasing private sector information sharing within the legal requirements of their domestic DPP framework. Each of these information sharing initiatives needs to be considered on a case-by-case basis depending on their unique characteristics and the relevant DPP requirements.

These experiences indicate that AML/CFT/CPF private sector information sharing measures can be achieved in compliance with DPP rules and obligations, subject to

key tests and requirements. While technology can play an enabling role in balancing policy objectives and reducing the privacy risks, adequate governance and legal frameworks are key to the success of these initiatives. As private information sharing initiatives are piloted or progress and mature, there will be more quantitative data to assess if, when and how this type of sharing can enhance AML/CFT/CPF effectiveness.

The FATF hopes that this work will assist countries that are considering embarking on private sector information sharing mechanisms to understand how their peers have addressed DPP obligations in designing information sharing initiatives.

This is a non-binding report. Its recommendations to jurisdictions that are considering enhancing information exchange among private sector entities reflect observations and lessons learnt across jurisdictions of the FATF global network::

- The public sector should consider taking an active facilitation role in private sector information sharing initiatives, for example by updating laws or supervisory instruments as necessary; making use of regulatory sandboxes and pilot programmes; highlighting areas, typologies or data types that would benefit from sharing; identifying a lead agency/contact point to promote collaboration and co-ordination; providing guidance or checklists; building secure platforms for sharing and oversight; and developing projects to harmonise and standardise data.
- The public sector should ensure and promote regular dialogue between DPP and AML/CFT authorities, consistent with the FATF Recommendation 2, as well as internationally, for example by holding regular forums; devising a joint strategy; providing joint guidance or conducting sector-wide engagement; providing assistance to industry initiatives; and conducting joint initiatives, such as regulatory sandboxes or technology sprints.
- The private sector should consider the application of privacy-enhancing technologies where they are fit for purpose; take steps towards data preparation; pursue data protection by design; establish early and ongoing engagement with DPP authorities; develop indicators and metrics to measure success; and adopt measures to prevent de-risking related to information sharing.

[1] The right to privacy is enshrined in international human rights instruments, albeit in slightly different formulations, including the 1948 Universal Declaration of Human Rights; the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms; and the 1966 United Nations International Covenant on Civil and Political Rights (ICCPR) (right to be free from arbitrary and unlawful interference with privacy). AML/CFT/CPF regimes help prevent criminal activity that violates fundamental human rights (e.g., helping to detect and prevent human trafficking, corruption, and terrorism). AML/CFT/CPF also contributes to achieving sustainable development objectives (e.g., UN Sustainable Development Goals target 16.4).

[2] Data protection bodies: the European Data Protection Board (Financial Matters Expert Subgroup) (including through its members); the Council of Europe (including the 108 Committee and the Data Protection Unit); the Global Privacy Assembly (Data Sharing Working Group); the OECD Working Party on Data Governance and Privacy and its Secretariat. National data protection authorities: the Department of Innovation, Science, and Economic Development of Canada; the Jersey Office of the Information Commissioner; the Luxembourg Data Protection Commission; the National Institute for Transparency, Access to Information, and Personal Data of Mexico (INAI); the Norwegian Data Protection Authority; the UK Information Commissioner's Office. Financial institutions and associations: Commerzbank; Lloyds; Santander; the European Banking Federation, Institute of International Finance, the Wolfsberg Group and financial institutions involved in UK, Singapore and Estonian focus groups. Technology or solution providers: Ant Group; Deloitte; FutureFlow; Duality; Elucidate; HAWK AI; Salv; and Transactie Monitoring Nederland (TMNL). Academics/Think Tanks or other experts: the Future of Financial Intelligence Sharing programme, Dr. Benjamin Vogel – Max Planck Institute, Dr. Eleni Kosta - Tilburg University; Ben Hayes – consultant to CoE; and Vivienne Artz – Project Rose. Various forms of feedback were provided, including written comments on drafts, invitation for FATF to present to relevant working groups or involvement in the FATF project team focus group discussions.

SECTION ONE: Introduction

1. In July 2021, the FATF published a Stocktake on Data Pooling, Collaborative Analytics and Data Protection (hereafter referred to as the "Stocktake Report"). The Stocktake Report recognises that privacy-enhancing and other technologies could support information sharing while protecting privacy and personal data. While these technologies have not currently been adopted at scale and their application will need to be considered on a case-by-case basis, the use cases covered in the Stocktake Report have outlined their potential in offering promising ways for private sector collaboration, while remaining in line with national and international DPP frameworks. Based on the stocktake results, the Stocktake Report highlighted the need for greater regulatory clarity, promotion of enabling environments, data standardisation and governance, and bias prevention in artificial intelligence for more effective AML/CFT/CPF information sharing within an appropriate DPP framework at both international and national levels. This report builds on those findings, by sharing lessons from across the Global Network on how certain countries have addressed these issues when designing and implementing information sharing initiatives.

2. Competent authorities (such as supervisors/regulators and law enforcement authorities) and financial institutions need access to certain information about customers and their financial transactions to protect individuals from fraud and other malicious financial activities, to protect the public and global financial markets, and to accomplish AML/CFT/CPF objectives, including by detecting, investigating, and prosecuting or otherwise sanctioning natural and legal persons for ML/TF. Feedback from the private sector during FATF mutual evaluations suggests that users of financial services are generally aware that the private sector accesses and uses personal data in line with relevant domestic and international obligations (e.g., to identify and verify customers' identities) in order to mitigate the risks of financial crime.[1] Increasingly, there is also an awareness that governments use the information in a lawful manner to advance public interest, including to protect society from crimes such as fraud, corruption, drug trafficking, human trafficking or terrorism by investigating the relevant financial trails.

[1] This refers to broad trends in societal expectations and does not override the legal right in many jurisdictions to be informed of any such use of their personal data. For example, this is the case in the EU.

3. A range of international conventions and treaties, international agreements, laws, regulations, and frameworks around the world grant individuals data protection and/or privacy rights. These rights provide the foundation for democracy and rule of law; indeed, data protection and privacy rights are essential for the effective exercise of other human rights and fundamental freedoms, such as freedom of expression, association, religion, and assembly.

4. As demonstrated in the case studies in this report, financial institutions in certain jurisdictions are exploring sharing information for AML/CFT/CPF purposes. Where one institution might struggle to identify a complex suspicious transaction pattern or network, information from other institutions may complete this picture. Conversely, additional information may help an institution determine that a transaction that initially appeared unusual, was not suspicious. It is imperative that any such exchange of personal data (such as customer data or personally-identifiable transaction data) among private sector entities be limited to what is necessary, reasonable and proportionate, in line with applicable legal frameworks. Where personal data is shared, DPP considerations and objectives should be built into the sharing initiative. Data sharing initiatives should be implemented on a case-by-case basis through policies, regulations, procedures or other arrangements designed to meet legitimate public interests of protecting society from criminal activities, including terrorism. This policy calibration, often supported by enabling technology, should seek to balance the need to disrupt criminal activities without compromising the policy objectives of relevant national and international DPP laws and legal frameworks.

5. There can be significant challenges in meeting AML/CFT/CPF objectives in an optimal manner, while protecting personal data and privacy. The specific data protection and privacy requirements, including the exceptions and exemptions, differ between jurisdictions. In 2021, 145 jurisdictions have some type of legislation in place to ensure the protection of data and privacy.[2] Through reviewing specific case studies in different jurisdictions governed by different sets of AML/CFT/CPF and DPP laws, this report explores how it could be possible to fulfil both sets of objectives. Building on the findings of the Phase 1 Stocktake Report and focused discussion for this second phase, this report highlights some common responses and solutions adopted by private sector entities, and at times by the public sector, in conducting effective information-sharing while working to meet both AML/CFT/CPF and DPP objectives and obligations. This report seeks to serve as a reference and provide lessons-learnt for interested stakeholders in both the public and private sectors who wish to introduce and develop data pooling/information sharing initiatives to promote AML/CFT/CPF effectiveness.[3]

6. The information sharing case studies detailed in this report are tailored to specific purposes and objectives, namely the detection of suspicious activity. In several initiatives, certain personal customer data and related transactions would be analysed by participating financial institutions for possible criminal activity and, following the detection of suspicious activity, the relevant financial institution

[2] G Greenleaf (2021) "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance", available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

[3] The FATF Standards set out specific requirements on private sector information sharing in certain situations. See Section 2 for more details.

would follow its usual policies and procedures. These include following up and investigating the situation, contacting the customer with questions, and/or submitting a suspicious transaction report (STR). While a number of these projects are at an early stage, they are designed to comply with relevant DPP requirements, while improving on AML/CFT/CPF outcomes. The information included in the report was collected through multi-stakeholder country-level focus groups and the final report has benefitted from feedback from data protection authorities, academics and other experts, technology providers and the financial sector.

7. Detecting, investigating, and prosecuting individuals for ML/TF while protecting individuals' data and privacy is not optional; it is essential that both are achieved, to protect public safety, global markets, and national security, and also protect democracy and the rule of law. Further, it is worth exploring whether information sharing initiatives supported by appropriate safeguards have the potential to further DPP objectives by: improving the accuracy of STRs, reducing false positives and related investigations, or reducing the amount of personal data being shared with authorities. This has been recognised by certain DPP authorities that have taken a proactive approach in facilitating or supporting private-to-private information sharing, while ensuring appropriate DPP safeguards are in place. For example, the UK Information Commissioner's Office (the DPP authority) recognised that the "collaborative approach to fighting financial crime opens up the prospect of higher detection rates with lower false positives, while reducing the burden of scrutiny on each individual and business consumer."[4] As private information sharing initiatives are piloted or progress and mature, there will be more quantitative data to assess if, when and how this type of sharing can enhance AML/CFT/CPF effectiveness.

8. In order for countries and private sector entities to effectively develop and implement private-to-private AML/CFT/CPF data sharing that is compliant with DPP laws, regulations and principles, it is important that each project is developed on a case-by-case basis. Each project also needs to be consistent with applicable requirements and based on the particularities of the initiative, while potentially borrowing elements from the use cases discussed in this report. Nonetheless, it will be helpful to outline what has worked in certain jurisdictions, and what has not worked, including some common objectives, standards and protocols that help enable private-to-private data sharing for the detection, reporting and ultimately the disruption of professional money laundering networks operating across different entities and jurisdictions.

[4] Report by the UK's DPP authority (Information Commissioner's Office (ICO)) on a regulatory sandbox undertaken by the UK's DPP authority, https://ico.org.uk/media/for-organisations/documents/2618552/futureflow-sandbox-report.pdf, page 3, point 1.2.

SECTION TWO:
What are the global requirements on AML/CFT/CPF and to what extent does private-to-private information sharing contribute to their effective implementation?

9. This section provides an introduction to the global AML/CFT/CPF requirements for non-AML/CFT/CPF experts. It gives a broad overview of private sector information sharing, and highlights the usefulness of such sharing, for ML/TF/PF prevention purposes. Later sections focus specifically on information sharing for the purposes of detecting or investigating potential suspicious transactions.

10. The FATF[5] Standards set out the global requirements for AML/CFT/CPF systems and provide a framework for operationalising international legal obligations contained in the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, 1988; the *United Nations Convention against Transnational Organised Crime*, 2000; the *United Nations Convention against Corruption*, 2003; and the *Terrorist Financing Convention*, 1999 and to implement United Nations Security Council Resolutions. They are the international standard on combating ML/TF/PF, and other related threats to the integrity of the international financial system. Over 200 countries have committed to meeting the FATF Standards and undergo detailed evaluations against these standards.

11. The FATF Standards set out a range of mandatory requirements that countries must impose on their private sector (through national law, regulations and other measures). These requirements are collectively referred to as 'preventative measures' and they form the basis for other efforts, including by regulators and law enforcement, to detect criminal finance. These requirements include the collection and retention of personal data (e.g., for identity verification purposes). Specifically on information sharing, the FATF Standards currently require information sharing within the private sector in the context of correspondent banking, processing wire transfers, relying on third parties and implementing group-wide AML/CFT programmes. In some cases, such information exchanges are automated, while in others they are manual. While there are no other mandatory FATF obligations for

[5] The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions with the mandate to set standards and to promote effective implementation of legal, regulatory and operational measures for combating ML, TF and PF, and other related threats to the integrity of the international financial system.

private-to-private information sharing in other circumstances, jurisdictions may implement additional information sharing initiatives in order to better deploy resources in a risk-based manner and develop innovative techniques to combat ML, TF and PF.

12. This report focuses on information sharing to support the submission of suspicious transaction reports (STRs)[6] to the Financial Intelligence Unit (FIU). An overview of the other requirements that may be relevant to information sharing is provided at Annex A.

STR requirements[7]

13. FATF Recommendation 20 (R.20) stipulates that if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF, it should be required to report its suspicions promptly to the country's FIU. The reporting requirement must be a direct, mandatory obligation, and any indirect or implicit obligation to report suspicious transactions is not acceptable under R.20.

14. The private sector must take a risk-based approach to mitigating the ML/TF/PF risks it faces. For example, to identify potentially suspicious activity, institutions may direct additional resources at those areas (customers, services, products, locations, etc.) that it has identified as higher risk. In order to comply with its requirements under R.20, the private sector must collect and share personally identifiable information with the FIU. The private sector is also required to identify and verify the identity of customers and undertake ongoing monitoring of their transactions/circumstances to ensure that their activities are in line with what they have reported and to have a basis on which to determine if their transactions may be suspicious. The private sector uses transaction monitoring systems, including common risk indicators (such as those provided by the FATF, government authorities or commercial providers) to identify potential suspicious activity across a range of crime types. This system is designed to ensure that the financial sector is not used to finance crime, terrorism, or to evade financial sanctions relating to terrorism and the proliferation of weapons of mass destruction.

15. As outlined in Phase 1 Stocktake Report, information sharing (both private-to-private and private-to-public) is critical to fight ML/TF/PF. Multinational criminal schemes do not respect national boundaries, nor do criminals or terrorists exploit only one institution to launder their ill-gotten gains or move or use funds with links to terrorism.[8] The Phase 1 Stocktake Report sets out the objectives and preconditions for private sector AML/CFT/CPF information sharing and analysis.[9] There are existing FATF requirements for information sharing between private sector entities[10] in the context of correspondent banking (Recommendation 13), processing of wire transfers (Recommendation 16) and in the context of

---

6 Sometimes referred to suspicious activity reports (SARs) or unusual transaction reports (UTRs) depending on national legislation.

7 Paragraphs 77 to 79 of the Phase 1 Stocktake Report have explained how STR confidentiality rules can create challenges for private-to-private information sharing.

8 See also para. 23 of the Phase 1 Stocktake Report.

9 See Section 4 of the Phase 1 Stocktake Report.

10 FATF (2016-2017), *Consolidated FATF Standards on Information Sharing*, FATF, Paris , updated November 2017,

implementing AML/CFT measures within a financial group (Recommendation 18). In addition, information sharing occurs to support other requirements including identifying and verifying customers or beneficial owners (Recommendations 10, 24, 25) and risk management (Recommendation 1), notably under public/private partnerships.

Box 2.1. Potential use cases that could support the fight against ML, TF and PF

As set out in the Phase 1 Stocktake Report, private-to-private data sharing outside financial groups is perceived as restricted in many jurisdictions, due to requirements relating to DPP and/or jurisdiction-specific fundamental rights. According to applicable national legislation and the need for AML/CFT/CPF risk mitigation, FIs may wish to share data, both within and outside financial groups and potentially across jurisdictions, to facilitate more effective customer due diligence measures and other financial crime risk-management objectives such as those set out below. The list below sets out why it could potentially be beneficial for private sector entities to share information for AML/CFT/CPF, as an important public policy objective. Their inclusion does not presume that these cases meet or comply with the relevant assessments, tests, or thresholds under DPP rules.

- **Customer identification/verification:** to verify customer identity; to identify if a natural or legal person has previously raised flags or concerns; to verify the risk rating of customers by checking the existence of similar customer behaviour across business lines.
- **Transaction monitoring:** to detect layering[11] by examining the transaction pattern of a customer in order to assess the financial profile; to follow-up on any abnormal activity detected within and across institutions; to better identify suspicious activity (or conversely, to better identify activity which is unusual, but not suspicious); to apply transaction thresholds.
- **Sanctions or other screening:** to screen customers and counterparties in transactions against United Nations and domestic sanctions lists (including on terrorist financing and proliferation financing). This can also including screening against lists of politically exposed persons or other lists provided by commercial service providers.
- **Risk understanding and 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

11 Layering occurs after illegal proceeds have been placed into the legitimate financial system. Funds are further legitimised and distanced from their criminal origin by going through additional transactions or financial instruments (layers).

a more efficient record-keeping of beneficial owner information.

- **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 inquiries**: to align pro-active inquiries into potential suspicious transactions and reach more definitive conclusions to aid FIU or law enforcement investigations.

16. In line with the applicable legal framework, countries or entities may decide that private sector information sharing is required to effectively mitigate the ML/TF/PF risks they face and in particular (for the purposes of this paper), to identify suspicious transactions. Based on various discussion the FATF has had with both the private and public sectors[12], it is increasingly difficult for a single private sector entity to identify suspicious transactions in complex schemes designed to avoid detection. The FATF and other stakeholders have reported on intricate ML/TF/PF schemes that involve complex legal arrangements and transaction patterns that are difficult or impossible to detect without information from counterparty banks or other banks providing services to the same customer or its associates. Furthermore, as the number of transactions grows, it may be increasingly complicated for transaction monitoring systems to pinpoint suspicious activity. Without the ability to access and process additional information among private sector entities, there is a risk that these systems may be capturing transactions which are not relevant, and reporting false positives as a result. Appropriately tailored sharing of data among financial institutions or with FIUs can lead to improved detection and reduction of false positives. As a result, legitimate customers and transactions would no longer be flagged as suspicious.

17. As demonstrated by in-depth discussion on certain use cases (see case boxes below), where entities undertake investigations into potentially suspicious clients or activity in silos, more data has to be collected and recorded because every individual entity has to perform investigations of its own and determine whether the transaction or relationship is suspicious. Information sharing among private sector entities may have the potential to assist customers (and authorities) to reduce data collection at different points and pinpoint suspicious activities with greater accuracy, leading to better AML/CFT/CPF outcomes and customer experiences if proper DPP safeguards are in place. With more focused data collection, private sector entities may also be able to reduce their operational burden in processing and analysing large amounts of low quality data that may not necessarily lead to the successful identification of a suspicious transaction.

[12] Such as FATF Joint Experts' Meetings and other engagement fora with the private sector such as the Private Sector Consultative Forum and other focus group discussions and high-level conference held as part of this project.

SECTION THREE:
What are data protection and privacy requirements and objectives?

18. This section provides an introduction to DPP requirements for non-DPP experts. A right to privacy is enshrined in the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*.[13] While the specific interpretation may differ from jurisdiction to jurisdiction, the right to privacy would generally include freedom from interference or intrusion and the ability to control who can see or use personal information.[14] This is where the right to privacy intersects with data protection. While the UN has called upon jurisdictions to put in place a legal framework to protect privacy, there is no single inter-governmental organisation with a global membership that establishes specific international standards for DPP laws. DPP requirements have evolved differently in different jurisdictions, reflecting historical and cultural experiences on the ground[15] and different applicable legal norms or frameworks. In many jurisdictions, DPP legislation generally requires transparency about data collections, uses, and sharing; restricts disclosure of records to situations where an individual has given free and informed consent[16] or where another lawful basis for sharing applies; and gives individuals a right of access to their data, right to amend or supress incorrect data, and a right to redress or remedies for privacy violations, with certain limited exceptions (e.g., for law enforcement and national security).

19. Inter-governmental organisations adopted DPP principles that provided the foundation for some national constitutions, laws, and regulations. In 1976, the United Nations developed the *International Covenant on Civil and Political Rights* (ICCPR), which directs governments to protect certain individual rights and

13 UDHR, art.12; ICCPR, art.17 (protection from "arbitrary or unlawful interference with … privacy").

14 Ibid; UN Resolution 73/179 (2018) The right to privacy in the digital age.

15 Significant breaches of DPP have impacted the way in which rules are currently interpreted. These breaches have been committed by both the public sector and private sector (e.g. tracking by technology companies for commercial or advertising purposes).

16 Free consent would generally require the individual to have a free choice and be able to refuse or withdraw consent without being put at a disadvantage. Other requirements relating to consent are set out in relevant national and international law, e.g., Convention 108+.

freedoms, with privacy as one of many rights.[17] The Global Privacy Assembly (GPA) first met in 1979 and has been a global forum for data protection and privacy authorities. The Assembly seeks to provide leadership at international level in data protection and privacy by connecting the efforts of more than 130 data protection and privacy authorities from across the globe.[18] The Organisation for Economic Cooperation and Development (OECD) adopted *Privacy Guidelines* in 1980 and revised them in 2013.[19] The OECD is currently convening a drafting group of country experts, including law enforcement and national security agencies, alongside privacy authorities, with a view to developing principles for government access to personal data held by the private sector for law enforcement and national security purposes.[20] In 1981, the Council of Europe (CoE), which plays a leading role in international privacy issues, adopted Convention 108. The Convention now has 55 signatories spanning three continents, and was recently updated to Convention 108+.[21] In addition, the CoE is currently preparing draft guidelines on data protection implications of exchanges for AML/CFT/CPF.

20. In the European region, the 1950 *European Convention on Human Rights*, specifies that there should be no interference by a public authority with the exercise of the right to respect for of private and family life, except such as in accordance with the law and is necessary in a democratic society (Article 8). The European Union (EU) adopted in 2000 its *Charter of Fundamental Rights*, which protects the fundamental rights to privacy (Article 7) and personal data (Article 8). It specifies that any limitation on the exercise of such rights must be provided by law, and that limitations may only be made if they are necessary and genuinely meet the objectives of general interest (Article 52). It also enshrines the principle of proportionality. In 2016, the EU adopted a comprehensive regulation on data protection that is directly applicable in Member States: the *General Data Protection Regulation* (GDPR).[22] The GDPR is supervised and enforced by the data protection

---

17 The ICCPR, in various articles, provides that individuals shall have the "right to liberty and security of person", "inherent right to life…protected by law", "liberty of movement and freedom to choose his residence,", "right to hold opinions without interference" and "right to freedom of expression", and "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". www.ohchr.org/EN/Issues/RuleOfLaw/CompilationDemocracy/Pages/ICCPR.aspx .

18 The GPA was initially known as the International Conference of Data Protection and Privacy Commissioners (ICDPPC), https://globalprivacyassembly.org/.

19 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, updated revised in 2013, https://www.oecd.org/sti/ieconomy/privacy.htm.

20 See e.g. OECD (2021), OECD Secretary-General's Report to Ministers 2021, OECD Publishing, Paris, https://doi.org/10.1787/8cd95b77-en; OECD (2020), Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy,

21 Convention 108+, Convention for the Protection of Individuals with Regard to the Processing of Personal Data, June 2018, http://www.coe.int/dataprotection.

22 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). At the same time, the EU adopted the Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. This applies where personal

authorities (DPAs) in each EU and EEA Member State. The European Data Protection Board (EDPB), which is made up of representatives from each DPA and the European Data Protection Supervisor (EDPS), ensures that the GDPR is applied consistently throughout the EU. The EDPS ensures that the EU Data Protection Regulation[23] (the EU counterpart to the GDPR) is implemented for EU institutions, bodies, offices and agencies.

21. In the Americas region, the *Principles of Privacy and Protection of Personal Data* (Organisation of American States, 2021) and the *Personal Data Protection Standards* (Ibero-American Data Protection Network, 2017) aim to identify basic elements of effective protection and establish a set of common principles for data protection in the region.

22. In addition to these multilateral frameworks, various national constitutions, laws, regulations, guidelines, and policies related to privacy rights also exist worldwide. Approximately 145 jurisdictions have some type of legislation in place to ensure the protection of data and privacy.[24] As noted above, EU member states are subject to the *EU General Data Protection Regulation* (GDPR). The UK GDPR and the *Data Protection Act* 2018 provide a regulatory framework for data protection in the UK that is comparable to the EU GDPR. In the U.S., the Constitution establishes the foundation for protecting privacy by prohibiting unreasonable searches and seizures, among other protections.[25] In response to concerns raised with the advent of computers and automated data processing, the U.S. developed the "fair information practice principles", which were implemented in the Privacy Act of 1974.[26] The *Privacy Act* governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies, and requires transparency concerning uses and dissemination of information, as well as remedies for violations.[27] Later U.S. privacy laws at the Federal and state levels have been specifically tailored to sectors and associated

---

data is processed by a competent authority for law enforcement purposes, so is not relevant for private-to-private information sharing.

23 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

24 G Greenleaf (2021) "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance", available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348

25 "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. 4th Am.

26 See Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare (July, 1973).

27 See Privacy Act of 1974, 5 U.S.C. § 552a; U.S. Department of Justice, Office of Privacy and Civil Liberties, Overview of the Privacy Act of 1974, available at www.justice.gov/opcl/overview-privacy-act-1974-2020-edition. Certain exceptions apply in the law enforcement and national security contexts. Privacy Act, 5 U.S.C. §§ 552a(j)-(k). Note that certain redress rights were extended to citizens of certain countries through the Judicial Redress Act of 2015, 5 U.S.C. § 552a note.

risks, for example, the Gramm-Leach-Bliley Act (as amended) imposes rules on the financial sector, including privacy rules, as enforced by the applicable U.S. financial regulators.[28]

23. While the type and scope of DPP requirements differ from jurisdiction to jurisdiction, a review of the laws and legal frameworks mentioned above and discussions with DPP authorities show that these frameworks often follow similar general principles, and establish oversight and accountability mechanisms to ensure that the safeguards are implemented and effective. Such principles may include:

- **Type of data:** DPP protections generally apply to personal data relating to natural persons, often defined with reference to concepts like identifiability (e.g., through a name, number, or location, or through a combination of identifying factors). Different categories of personal data may also exist (either within or outside the legal framework).
- **Lawful authority (or "lawful basis"):** In certain jurisdictions (e.g. EU), **t**here needs to be a legal basis for processing personal data. Under the GDPR there is a finite list of legal bases for using/processing personal data, including: data subject's free consent to the processing for one or more specific purposes; processing necessary for performance of a contract; for compliance with a legal obligation; for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or for a legitimate interest (unless, on balance, there is a good reason to protect the data), subject to necessity and proportionality requirements. To use the 'legitimate interest' ground, data controllers (the person or entity that determines the purposes and means of processing)[29] would generally need to identify a legitimate interest, show that processing is necessary to achieve it, and balance it against the individual's interests, rights and freedoms.
- **Purpose and use**: The data should be processed/used in line with the specified, legitimate purpose and not used for any incompatible purposes. The processing of personal data should be done for a specific, well-defined purpose and data should not be further processed or used for additional purposes unless this is permitted and/or compatible with the original purpose.
- **Necessity, reasonableness, proportionality, and minimisation:** Even where there is a lawful basis for processing data, in certain jurisdictions the processing of the data should be necessary and reasonable or proportionate to that purpose. For example, depending on the jurisdiction, this may mean that: data should be retained only for as long as necessary; the information collected should be reasonable and not excessive in relation to the purposes for which it is processed;

---

28 Gramm-Leach-Biley Financial Services Modernization Act, 15 U.S.C. §§ 6801, 6809, and 6827 (1999).

29 The GDPR defines a data controller as a natural or legal person which alone or jointly with others determines the purposes and means of processing (art. 4(7)). The status as controller impacts the legal obligations and potential liabilities in the event of violation.

or there should be no other reasonable and less intrusive way to achieve the purpose. Institutions should consider to what extent their aims can be achieve *without* the sharing of personal data (e.g., by using available anonymisation technologies).

- **Quality and integrity**: Personal data should be maintained in such a manner that the data is accurate, reliable, complete, consistent and in context. This could include an obligation to keep data as up to date as is necessary and appropriate for the processing of the data, with regard to the purposes for which it is processed.
- **Fairness, including in automated decisions:** Processing must be fair and lawful. Decisions that can have a significant adverse impact on an individual's interests should not be made solely on the basis of the automated processing of the personal data, unless otherwise authorised under domestic law and subject to appropriate safeguards. Depending on the legal framework, this may apply only to the extent that the adverse impacts are related to the purpose for which the data is processed, or more broadly. In some jurisdictions automated decision-making is prohibited unless specific conditions are met.
- **Transparency**: Data subjects should be informed about, among other things, how and by whom the data will be processed, for which purpose, to what extent the personal data are or will be processed; individuals and relevant authorities should be notified of data breaches.
- **Data transfers/disclosures:** In certain jurisdictions, transfers or disclosures of data with another organisation can only occur with prior free consent, which can be withdrawn at any time. Other jurisdictions may permit transfers/disclosures pursuant to a specific legal basis (regardless of consent) and in accordance with specific restrictions set out in law to ensure continued protection of the data, necessity and proportionality.
- **Data Security**: Personal data must be processed using appropriate physical, technical, and organisational measures to protect the data, in particular against unauthorised or unlawful processing and accidental loss, destruction or damage, and records should be maintained to demonstrate how personal data is accessed, used, and disclosed, e.g. computer audit logs.
- **Access, correction and other data subject rights**: There should be procedures in place for individuals to be informed and to seek and obtain access to the data, and to request correction of data that the individual asserts is inaccurate, or erasure in certain jurisdictions, subject to reasonable restrictions under domestic law, e.g. law enforcement and national security purposes. Depending on the applicable framework, other data subject rights may include the right to suppress or erase data, the right to restrict processing, and the right to data portability (i.e., the subject's right to receive personal data from a controller in a structured, commonly used and machine readable format).

- **Accountability/Oversight:** The use and processing of data should be reviewed by one or more bodies that exercise functionally independent and effective oversight, either alone or cumulatively.
- **Redress:** There should be appropriate and effective mechanisms to enable an individual to submit complaints and to seek redress. Subject to reasonable restrictions imposed by domestic law, mechanisms should include the receipt and investigation of complaints made by an individual to whom the personal data relates and who seeks redress with respect to access, the correction, or an alleged improper processing of the data. In certain jurisdictions, this may include judicial redress before courts operating in accordance with the rule of law.
- **Impact assessments**: In many jurisdictions, laws, regulations, or policies require an institution to assess the data protection and privacy risks to individuals from the proposed collection, use, dissemination, or other processing of personal data, and implement ways to minimise such risks.[30] For example, under the GDPR, this assessment and mitigation of risks is documented as a 'data protection impact assessment' (DPIA), while in the U.S. federal agencies must complete a 'privacy impact assessment'.[31]

24. DPP laws and frameworks generally also contain **exceptions, exemptions, restrictions, or limitations to privacy rights in certain situations**, including for purposes of prevention, investigation, detection or prosecution of criminal offences. These might apply only to specific offences, such as fraud or terrorism. Even in such cases, as a general rule, stakeholders should, to the extent applicable, be encouraged to bear in mind the DPP principles set out above when designing private sector information sharing initiatives. By doing so, they are likely to reduce the DPP risks, particularly for entities active in multiple jurisdictions, and build greater public trust in these initiatives.[32]

---

30 Additional impact assessments may also prove useful in identifying and mitigating other types of risks. See para.59, Section 6 below (on Human Rights Impact Assessments, Legitimate Interest Assessments).

31 See GDPR Art. 35; E-Government Act of 2002, Pub. L. 107-347 (2002), Section 208.

32 For example, in the U.S., the Department of Justice has developed and maintains practices and procedures for the law enforcement and national security contexts to protect personal data and mitigate risks, e.g., the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, the Justice Manual, the FBI DIOG, updated frequently to reflect new laws and rules of procedure, executive orders, internal policies, best practices, and new information technologies. *See* E.O. 12333, Section 2.3; Justice Manual (JM) (2018); Federal Bureau of Investigation, Domestic Investigations and Operations Guide (DIOG) (2016).

SECTION FOUR:
Presentation of information sharing case studies

25. The following case studies are examples where entities and authorities have endeavoured (or are in the process of endeavouring) to balance AML/CFT/CPF and DPP objectives, while operating within the applicable legal framework, to advance private sector information sharing for AML/CFT/CPF. Most of these projects have been designed, implemented, and co-ordinated with both AML/CFT/CPF and DPP authorities. While digital transformation assisted in these examples, they also required other measures. While most examples relate to sharing for AML/CFT purposes, one example on information-sharing in a fraud-context is also included as it involved a certification/approval regime by a DPP authority (see Box 4.4 below) and is a useful illustration of similar initiatives.

26. The case studies reflect different scenarios, each with its own analysis of DPP rules: (a) data sharing and analysis of large volumes of de-identified/pseudonymised/encrypted information aimed at identifying suspicious transactions (referred to as **pre-suspicion information sharing**), and (b) narrow, targeted information sharing to advance specific investigations, using personally identifiable information related to suspicious transactions (referred to as **post-suspicion information sharing**). Depending on the regime, and as illustrated by the case studies below, these two types of sharing will involve different DPP considerations; with pre-suspicion sharing generally being subject to stricter limitations, in line with individual privacy rights.

27. Most case studies focus on information sharing within the private sector (i.e., financial institution to financial institution), but some include sharing with public sector authorities.

28. The case studies below are based on information provided by the authorities and institutions involved or publicly available information. The legal reasoning and facts presented in the case studies represent the views of the relevant jurisdictions/stakeholders rather than the FATF.

Box 4.1. TriBank pilot (following the FutureFlow Information Commissioner's Office (ICO) Sandbox) (UK): pre-suspicion private-private information sharing

Use case: The TriBank pilot involved pre-suspicion information sharing in bulk of transactional data that has undergone pseudonymisation in bulk, that is: transactional data with pseudonymised account identifiers to identify clusters/typologies

Participants:

- The TriBank pilot was led by a consultancy and involved three UK banks (the data controllers) and one technology provider (FutureFlow, the data processor (the person or entity that processes personal data)).[1]
- Prior to the pilot, the UK DPP authority (the Information Commissioners Office (ICO)) engaged with the data processor, FutureFlow, and considered key data protection issues arising from this operating model in a "regulatory sandbox" environment.[2]

Specific purpose/goal: The Tribank pilot aimed to improve detection of linked transactions that were unusual and could indicate potential ML/TF. When a transaction was flagged as unusual, the relevant bank would re-identify the transaction and, consistent with its usual policies and procedures, investigate further, and if warranted, submit a STR.

Specific data points collected/shared: The TriBank pilot used pseudonymised historical transactions of small to medium enterprises over a year. Using pseudonymised data minimised data protection and privacy risks, but because it could be re-identified, the data was considered personal data under the applicable legal framework. The technology highlighted transaction patterns that may have been high risk or unusual, and the banks were then able to re-identify their own data to investigate further and determine whether there were grounds for suspicion. The following categories of personal data were included after pseudonymisation: account identifier (such as account number, sort code, IBAN number, etc.); transaction value(s); transaction IDs; and time-stamps**.**

Lawful basis for processing personal data: During the TriBank pilot, each bank (the data controllers) needed to decide, in accordance with its domestic law, which lawful basis applied based on the data that the banks proposed to share. In this project, the banks shared only pseudonymised transaction data pre-suspicion. Once a participating bank detected an unusual or higher risk transaction pattern, the banks would share only narrowly-focused targeted information in order to investigate specific activity as necessary.

- The FutureFlow/ICO sandbox (prior to the TriBank pilot) had suggested that the most appropriate lawful basis was likely 'legitimate interest' (Article 6.1(f) of the GDPR[3]). The ICO issued a public opinion to this end in a sandbox report (as well as in associated communications).
- Participants in the pilot also explored 'compliance with a legal obligation' (Article 6.1(c) of the GDPR[4]) as a possible lawful basis to share, collate, and commission the analysis of the pseudonymised transactional data. However,

in this situation it was unlikely that sharing of data on the broad underlying account base, prior to any firm indication that accounts had been involved in suspicious activity (i.e., at the pre-suspicion stage), would be considered a reasonable and proportionate way of achieving compliance with the specific legal obligation. Rather, participants felt that it may be more appropriate for any *further* information sharing by the banks (i.e., to support investigations alerted by the FutureFlow platform) to rely on this lawful basis to undertake cross-institutional investigations as this further information sharing would be limited to just those accounts subject to an identified suspicion.

Assessment of proportionality: The data shared during the TriBank pilot related only to small to medium enterprises (legal persons) and was pseudonymised, which minimised DPP risks. The relevant clusters, once identified, could only be re-identified by the specific individual banks that originally submitted the data (the data controllers). The banks would properly investigate any reports which indicated that financial crime may have taken place, consistent with applicable financial legislation and internal bank policies/procedures. This investigation would occur before suspects experienced any changes to their level of service (i.e. suspects do not have their banking services removed purely on the basis of a finding/report by the common platform).

Technologies utilised: A sample of transactional data was pseudonymised using a hashing convention and placed in a common platform (AML utility). The platform cleaned and de-duplicated the pooled dataset and applied analytics algorithms to map out complex non-linear cross-bank account relationships in order to identify potential 'pre-suspicions' to be further investigated by the individual banks.

Involvement of authorities (AML/CFT/CPF and/or DPP): While not involved in the TriBank pilot, the UK DPP authority, the ICO, had worked with FutureFlow (the technology provider and data processor) as part of the sandbox environment to assess data protection risks and determine ways to mitigate these by way of a data protection impact assessment (DPIA)[5]. As part of this work, the ICO had issued a public opinion on the basis for processing.

Results:

- The TriBank pilot 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. However, following investigations by the banks involved, these clusters of activity were explainable in a number of cases. This suggests that analysis of pseudonymised transaction data alone is unlikely to be able to deliver the required information for detecting ML or that further work is required to better integrate known ML typologies or other intelligence feeds and technology/solutions in order to pinpoint suspicious clusters of activity.
- The technology provider envisaged an operating model with a two-tier DPP framework. The first phase would be based on legitimate interest and include bulk pseudonymised data (thereby protecting the privacy of the majority of customers who are not implicated in the typologies identified). However, once a typology or cluster or abnormal activity or pre-suspicion is formed, further

information sharing of individual account information could be based on compliance with law (to investigate and submit suspicious transaction reports or a legal gateway provided in AML/CFT/CPF or relevant legislation).

Source: Discussions with and input from the TriBank project participants, *Regulatory Sandbox Final Report: FutureFlow (October 2020)*, available at: https://ico.org.uk/media/for-organisations/documents/2618552/futureflow-sandbox-report.pdf

Notes

1. The GDPR defines a data processor as a natural or legal person which processes personal data on behalf of a controller (art.4(8)). The status as controller or processor impacts the legal obligations and potential liabilities in the event of violation.
2. A regulatory sandbox is a mechanism to allow firms (e.g., technology providers) to test innovations and conduct live experiments, generally in a limited and time-bound manner, in a controlled environment under a regulator's supervision. The TriBank pilot was not conducted within the sandbox, but after the initial sandbox testing.
3. The sandbox concluded in November 2020, at which time the UK was still subject to the GDPR under EU law. The applicable provision under UK law is article 6.1(f) of the UK GDPR.
4. And Article 6.1(c) of the UK GDPR.
5. A DPIA is required where an initiative is likely to involve "a high risk ti the rights and freedoms of individuals" (GDPR, art.35; UK GDPR, art.35).

Box 4.2. COSMIC (Singapore): pre-STR and post-STR public-private information sharing initiative

Use case: COSMIC is a secure digital platform, owned and operated by the Monetary Authority of Singapore (MAS), Singapore's financial supervisor. It is an information sharing initiative for risk discovery and data analytics collaboration. It will allow participating financial institutions to share customer information to assess suspicion and warn each other of potentially suspicious activity, where the customer's profile or behaviour crosses materiality "red flag" tests in priority risk areas. [1] The information shared will include risk analysis, customer or transaction data. Private-sector information sharing under the initiative will initially be permissive/voluntary, but MAS plans to make sharing mandatory in higher-risk situations after an initial phase to stabilise implementation of the platform.

Intended outcomes/results or achieved results: Currently, financial institutions (FIs) are not permitted to warn each other about potentially suspicious activity involving their customers, as they are not allowed to share customer information indiscriminately with each other due to concerns about information security and customer privacy. Criminals have been able to exploit this weakness by conducting transactions through a network of entities holding accounts with different FIs. As such, each FI by itself would not have sufficient information to detect and disrupt illicit transactions in a timely manner. Allowing FIs to share information on customers that cross material risk thresholds of strong probative value, breaks down these information silos and enhances detection of illicit networks and actors, increases disruption of criminal activity in priority risk areas, and supports cross-border disruption and deterrence of criminal behaviour. The

COSMIC project participants are discussing specific key performance indicators to measure the project's success.

Participants: MAS is co-developing COSMIC along with the Commercial Affairs Department (CAD) of the Singapore Police Force, and six major banks which will be its initial users. MAS has also worked closely with the Personal Data Protection Commission (PDPC) to ensure that sharing of information on COSMIC is in line with PDPC's principles for use of personal data.

As AML supervisor, MAS will integrate the platform data with its own supervisory surveillance and ensure that FIs use COSMIC appropriately. The Suspicious Transaction Office (STRO), Singapore's FIU, will have direct access and be able to use the information obtained from COSMIC for its own analytics.

Mode of information sharing:

- Where a customer has exhibited some red flag behaviour and an FI requires more risk information to assess whether there are reasons to suspect that its customer is involved in illicit activity, it may ***request*** risk information on the customer from other FIs which are linked to the activity.
- Where the customer's unusual activities cross a higher risk threshold, indicating a greater risk of the customer being involved in illicit activity, an FI would have to proactively ***provide*** risk information on the customer to other FIs with a link to the customer's activities.
- Where a customer's activities exhibit the higher threshold of red flags, and the FI has filed an STR on the customer and decided to terminate the relationship, the FI should place an ***Alert*** on this customer on the "watchlist" in COSMIC.
- In the initial phase, sharing information on COSMIC via ***Request, Provide*** and ***Alert*** will be non-mandatory. Thereafter, MAS expects that sharing of risk information via ***Provide*** and ***Alert*** will be made mandatory. It will also be mandatory for participating FIs to respond to ***Request*** messages after the initial phase.

Lawful basis for processing personal data: The Personal Data Protection Act (PDPA) provides a legislative route for other written law to prevail over the PDPA requirements. In this regard, MAS is making legislative amendments to the Financial Services and Markets Act to set out a regulatory framework for COSMIC. It will provide for the sharing of risk information between FIs for AML/CFT/CPF purposes. Specifically, the sharing of risk information between FIs will be permitted only between FIs that are participating on COSMIC, and within the bounds of the prescribed information sharing modes of "Request", "Provide" and "Alert".

For more information on the MAS consultation paper on the proposed information sharing platform and regulatory framework, please refer to: Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf (mas.gov.sg).

Specific data points collected/shared: Risk analysis, transaction, and customer information. For example, information on the customer could include particulars of directors, authorised signatories or beneficial owners (such as their name, date

of incorporation or birth, residential and/or business address, nationality or place of incorporation, and unique identification number). Transaction data or other red flag information could also be shared.

Participating FIs are required to share information using pre-defined data templates. The data template design includes:

- Case and FI identifiers
- Red flags identified and risk description
- Customer profile: Name, Incorporation/Business Registration Number, Date of Incorporation/Registration, Nature of Business, Place of Incorporation/Registration, etc.
- Account profile: Account type, status and open/closure date
- Transactional details: Originating and Beneficiary Names, account numbers, FIs, Date, Amount and Currency
- Details of customer(s) placed on an alert list and reasons for inclusion

Assessment of proportionality: Information sharing is initially targeted at three priority risk areas identified as part of the national risk assessment process and AML/CFT/CPF strategies. These three priority risks are: the misuse of legal persons, trade-based money laundering and proliferation financing. These are complex forms of financial crime which underline the need for information sharing. In order for information sharing to occur within COSMIC, a customer's behaviour or profile must exhibit multiple red flags or indicators of sufficient materiality and therefore be probative of financial crime concerns.

Other DPP considerations: As the purpose of COSMIC is for participating FIs to assess suspicion regarding a customer and warn each other of potentially suspicious actors, notifying the customer that their information is being shared could lead to criminals being tipped off that their illicit activities have come under scrutiny. On the other hand, to protect the interests of legitimate customers COSMIC has several layers of safeguards to ensure that customer information is appropriately shared, used and protected.

Firstly, FI must assess whether the customer has crossed the stipulated materiality risk tests, based on probative combinations of red flags the customer exhibits, before initiating risk information sharing via COSMIC. This will ensure that relevant information is shared precisely for AML/CFT/CPF purposes and in a proportionate manner, to enable an FI to examine whether there are reasonable grounds for suspecting its customer of illicit activity, or warn other FIs that a customer is engaging in potentially suspicious behaviour. An FI responding to a request for risk information from another participant FI will also be required to make an assessment and be satisfied that the requested risk information may assist in the assessment and determination of ML/TF/PF risk concerns before sharing such risk information.

Next, the legislative framework for COSMIC will prescribe safeguards on the use and confidentiality of information obtained from the platform, and require FIs to guard against inappropriate sharing of platform information. There will also be requirements to ensure that the information disclosed on the platform is accurate

and complete, and to promptly notify MAS and other relevant participant FIs of any error in the information provided, and to rectify such error as soon as possible.

Lastly, FIs will also be required to put in place a process for reviewing customer relationships, including providing the customer an adequate opportunity to address its concerns prior to existing a customer relationship. FIs should not rely solely on the information received from COSMIC, but should instead review the customer relationship holistically, taking into account other sources of information including the customer's explanation before deciding on whether to exit the customer relationship. Customers already have pre-existing channels, provided in law, to correct customer information that FIs collect from the customer such as identity information, and this avenue remains available to the customer with his bank and updated into COSMIC.

Data transfers/disclosures

FIs and their officers will not be permitted to disclose information obtained from COSMIC to any other person, except for the scenarios as expressly provided in legislation. Any further disclosure of platform information must be strictly in line with the principle that information shared should be relevant, proportionate and necessary for the purposes of assessing ML/TF/PF risk. For instance, FIs may need to disclose platform information for specific operational purposes, to facilitate the performance of ML/TF/PF risk management duties and outsourcing of ML/TF/PF risk management operational functions. FIs may also need to disclose platform information to local and overseas affiliates for group-wide ML/TF/PF risk management purposes, to strengthen group-wide risk mitigation and prevent bad actors from moving between entities within the same financial group. FIs disclosing platform information to prescribed persons for such purposes will be required to comply with additional safeguards, to mitigate against the risks of leakage and unauthorised disclosures, and unintended legal risk to FIs that had shared the information.

Confidentiality/data security

Participating FIs should appropriately classify COSMIC-related data and implement info-security measures to prevent any data leakage. As a baseline, they should ensure compliance with MAS requirements on data storage and protection:

- *Technology Risk Management Guidelines*, which comprise industry best practices that MAS expects FIs to adopt.
- *Notices on Technology Risk Management and Cyber Hygiene*, which set out requirements for FIs to adopt the necessary IT controls and cyber hygiene practices.

COSMIC-related data should be stored in a secure environment with appropriate encryption. COSMIC data should not be stored on individuals' laptops unless exceptionally warranted. Audit logs will be required for any viewing, editing or downloading of information involving sensitive data.

Technologies utilised: Information will be shared in a structured format, and on an online platform that includes security features such as user-authentication mechanism and data encryption as well as entity resolution and network linked analysis. MAS will also use COSMIC information as part of its broader

AML/CFT/CPF analytics surveillance framework to identify illicit networks and emerging trends.

Additional considerations/challenges: MAS is cognisant that strengthening collaboration amongst an initial group of participant banks may raise the risk of illicit actors shifting their activities to FIs that do not participate on COSMIC. To address this risk, MAS is strengthening its surveillance to uncover such "risk migration" scenarios, and stepping up its supervisory engagement of FIs that are not on COSMIC, to warn them of such instances and provide guidance to tighten their AML/CFT/CPF controls. MAS and CAD will also continue collaborating with FIs on priority ML/TF investigations through the AML/CFT/CPF Industry Partnership (ACIP) and involve non-COSMIC FIs in such investigations, where warranted.

Source: Discussions with and input from COSMIC project participants, *MAS and Financial Industry to Use New Digital Platform to Fight Money Laundering* (October 2021), available at: *https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering*

Note
1. The initial three priority risk areas are misuse of legal persons, trade-based money laundering, and proliferation financing.

Box 4.3. Transaction Monitoring Netherlands (TMNL): pre-suspicion private-private information sharing initiative

Use case: Transactie Monitoring Nederland (TMNL) is an initiative of five Dutch banks in which TMNL aims to deliver faster, better, more effective transaction monitoring (TM), and as such enhance the formal role of banks as 'gatekeeper' to the financial system. The long-term ambition is to ultimately create an industry-wide utility for transaction monitoring, leading to better detection of money laundering and terrorist financing by financial institutions and delivery of higher quality information to law enforcement.

After its founding in July 2020, TMNL currently operates in the 'Minimal Viable Product' (MVP) stage. The objective of this stage is to improve the detection of money laundering by identifying unusual transaction patterns that individual banks cannot identify alone (so-called 'multibank alerts'). In this MVP stage:

- All activities by TMNL are on top of regular AML/CTF procedures conducted by its founding banks;
- Focus is on 'multibank' monitoring and detection of financial crime patterns that span accounts at multiple banks;
- TMNL is in the MVP stage a detection utility only, all alert review and client measures (including filing of Unusual Transaction Reports to FIU) are conducted by banks;
- The client scope is business entities only;

- Privacy sensitive data items are pseudonymised.

In the core operational process, banks transfer pseudonymised transaction data to TMNL. Based on advanced analytical models developed by TMNL specifically for the purpose of multibank transaction monitoring, alerts on potential unusual transaction patterns are generated. The individual entities that are part of such a potential unusual pattern (or 'case') are alerted by TMNL to the banks for review. As the required client information to perform the alert review is only available within banks, this alert review process is currently conducted within the bank environment.

Intended outcomes/results or achieved results: The current objective is to identify potentially illicit money flows and patterns that span multiple banks, and that cannot (by any feasible means) be uncovered by the respective banks in isolation because they can only see one piece of the puzzle. This is under the presumption that money laundering organizations typically, deliberately and increasingly create complex schemes to hide the origin and target of funds across a web of banks and bank accounts. Initial testing in a Proof of Concept, as well as the initial outcomes generated by the first alerts on several advanced analytics models TMNL has now generated, confirmed that numerous of such multibank cases were found of which a subset has been reported by the banks to the FIU.

Participants: TMNL is an initiative of five Dutch banks: ABN Amro, ING Bank, Rabobank, Triodos Bank and De Volksbank. All banks are shareholders to the TMNL legal entity, which is formally a fully private initiative. In practice, the Dutch banks work closely with their government partners to achieve sufficient consensus on several strategic and regulatory matters. Moreover, there is alignment with law enforcement on AML intelligence and typologies that can could be translated into the analytical models aimed at detecting multibank patterns of potential unusual transactions.

Mode of information sharing: Banks prepare transaction data for sharing within their own environment, this includes pseudonymisation of all data items that could directly or indirectly be related to individual entities (see also below). TMNL pools and relates the dataset of participating banks in analytical models performed at its highly secured IT platform. The alerts sent back to banks include a specific ID that only the respective receiving bank can relate back to its own client records. This translation process has to be performed at the bank before the bank investigators can review the TMNL alert.

Specific data points collected/shared: The current data scope of TMNL is restricted to business entities only, limited to what is required for TMNL's objectives and possible within the current legal frameworks. The scope includes transaction information (such as account number, transaction type and amount) as well as limited account and client information (such as IDs, account and client type, client industry). Due to the pseudonymisation scheme that is currently applied (see below), TMNL cannot identify individual clients in the datasets of the banks. As such, TMNL can only alert banks on the (multibank) transaction patterns it observes.

Use of privacy enhancing or other technologies: Although the current scope is limited to business entities, privacy measures are applied to preserve

confidentiality of the data that is processed. The assumption of the banks and TMNL is that some data could be personal data, and therefore TMNL treats all data as personal data. A key technique is pseudonymisation, in which all data items that could be related to individual clients (such as IDs, account numbers, names) are transformed into 'hashed' values. A set of private keys are used for this hashing process, which are preserved by a third party and in secured modules in the data preparation process. Since the secret keys are common across banks, transaction data can still be interrelated by TMNL based on pseudonymized data items that are also common across banks (for example the chamber of commerce number of a client, as well as an account number). So although client identity and information is unknown to TMNL, it can still analyse transactions across banks.

Lawful basis for processing personal data: To enable TMNL to fully operate collective transaction monitoring activities, the Ministries of Finance and Justice are working on an amendment of the Dutch AML/CTF Act. This amendment is part of the Dutch Government's National Action Plan against Money Laundering. Among other measures, 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. In anticipation of this amendment, TMNL has started with a limited scope of clients based on legitimate interest. As part of the creation process, extensive legal analysis was done to assess what and how data processing could fit within the current legal frameworks, pre-amendment.

Addressing DPP considerations: As part of a 'privacy by design' approach, a Data Protection Impact Assessment (DPIA) is conducted by the banks (being the data controllers) and TMNL (data processor) to assess GDPR key principles. Important data privacy and security measures are also formally agreed upon in the user agreement between TMNL and banks. Moreover, privacy considerations per analytical model are separately made, aligned and documented.

The starting point for the DPIA and related privacy considerations is the legitimate interest of the participating banks as controllers to enhance their formal role as gatekeeper to the financial system, and as such better act upon legal AML requirements. Supported by these AML requirements, the necessity to process data to achieve this goal of a better multibank detection, considerations that have also been described in the aforementioned National Action Plan against Money Laundering, as well as confirmations (by means of testing) that TMNL could enhance AML effectiveness for the participating banks, careful considerations around proportionality of the data processing have been made and aligned. Critical to these considerations are also the principles of purpose limitation and data minimisation.

In the execution of TMNL, a wide array of measures have been taken and tested to ensure accurate and secure data processing. Data quality analysis and remediation processes are performed both by banks as well as on a TMNL level to assess suitability of usage of the items in analytical models. The data itself cannot leave the TMNL IT platform to any other (external) party. The TMNL IT platform is subject to the highest IT security standards, including assessment, continuous

monitoring and testing of security measures. And the working of the analytical models is governed by a model risk framework aimed at ensuring valid, reliable, fair and transparent analytical models.

Additional considerations/challenges: The TMNL utility concept has been a pioneering initiative, from which it becomes clear that the current legal framework provides possibilities for data sharing but also implies important restrictions and uncertainties. TMNL has currently adopted an operating model that is possible within these restrictions and is conservative in dealing with the uncertainties, but that does not yet enable full AML effectiveness. For potential next steps on the roadmap towards a full transaction monitoring utility, restrictions and uncertainties from AML and privacy law are blocking. In order to enable utilities like TMNL to proceed and reach full effectiveness in the fight against financial crime, more legal clarity and certainty on data sharing as well as the tension between AML and privacy legislation will be required. If international regulations would provide more clarity on the definitions and boundaries for a utility concept that will encourage private and public actors to foster innovation and collaboration and come to a next level in their efforts to enhance the role of the banks as gatekeeper and combat financial crime together. Practically, if AML standards would describe more precisely what information could or should be shared for both AML detection and review processes, this could enable both deeper analysis with better outcomes, as well as less data processing and impact on low risk actors.

Involvement of authorities (AML/CFT/CPF and/or DPP): To operationalise the TMNL initiative, the Dutch banks are in close dialogue with a number of public partners. Authorities are currently involved to develop legislation to further support this initiative.

Source: Discussions with and input from TMNL project participants, *What is TMNL?* (2022), available at: *https://tmnl.nl/summary-eng/*

Box 4.4. Incident Alert System (IAS) for Financial Institutions (Netherlands): Post-suspicion sharing related to fraud

Use case: Post-suspicion sharing of identifying information on persons involved in fraud incidents, based on an initial hit/no-hit alert system, to detect potential customer risks.

Intended outcomes/results or achieved results: The IAS was established in 1997 to allow participating financial institutions (FIs) to help each other identify and prevent fraud. The system allows FIs to alert each other to customers, employees or other persons involved in incidents of fraud and facilitates the investigation of possible fraud. Since 1990, FIs' Security Departments have recorded incidents of fraud on an internal incidents register. In 1997, under the IAS, certain elements from the internal incident registers are included on an external register, which is accessible to other participating FIs on a hit/no-hit basis.

Participants: The IAS is open to all FIs that are members of a recognised trade association (i.e., the Dutch Banking Association; Association of Insurers; Association of Financing Companies in the Netherlands; Mortgage Fraud Prevention Foundation or Health Insurers Netherlands). Banks that are not members of the Dutch Banking Association and insurance entities that are not members of the Association of Insurers can be admitted as participants on a case-by-case basis.

Each participating FI remains the data controller. The IAS is managed by the *Credit Registration Bureau* (BKR) for data from other financial institutions, and the *Central Information System Foundation* (CIS) for data from insurance entities. These entities manage the external register and act as data processors.

A Guidance Committee (made up of representatives from some participating institutions) oversees the operation of the register to ensure uniform application and respect for the rules.

Mode of information sharing: Data is shared via an external register on which FIs record data on customers/employees/persons involved in fraud incidents. Information is included on the external register only where:

a) The person involved violated or attempted to violate a law, posing a threat to the interests of the FI's customers or employees, the FI itself, or the financial sector as a whole; and

b) There are sufficient grounds to establish that the identified individual was involved such that a criminal complaint or report will be or has been made (or would be made, if this action was not disproportionate to the offence or would have undesirable effects for law enforcement); and

c) The principle of proportionality is observed.

The IAS allows participating FIs to search the external register on a hit/no-hit basis to alert the consulting FI to fraud incidents involving the searched person. The IAS

also provides for retrospective hits – where a query results in a hit in the subsequent two months, the consulting FI will be alerted to the new entry. Where a hit is received, FIs can make a request for additional data to understand why the customer was entered on the register. These requests are considered on a case-by-case basis by the requested FI. Any exchange must be adequate, relevant and limited to what is necessary for the purpose of access.

Specific data points collected/shared: The external register contains identifying data on individuals involved in the fraud incident, e.g., name, address, date of birth, nationality, IBAN. However, initial consultation of the ERR is based on a hit/no-hit system, meaning no identifying data is shared upon first consultation. Instead, if there is a hit, the FI's Security Department must determine whether to seek further information, taking into account DPP requirements.

Lawful basis for processing personal data: Data sharing under the IAS is permitted under the GDPR for the legitimate interest of the detection and prevention of fraud (art.6(1)(f)). The Dutch General Data Protection Act (UAVG) requires the certification of any processing of personal data. The IAS has been certified, which required an assessment of the system by the DPA for compliance with DPP requirements.

Assessment of proportionality: Data sharing under the IAS is limited to a narrowly-defined group of FIs. The exchange of information is initially limited to a hit/no-hit basis. Additional sharing of information occurs only when necessary and is considered on a case-by-case basis by the requested FI's Security Department, which is required to consider whether the sharing is proportionate. Participating FIs are obliged to delete data from the register where it is no longer relevant (e.g., where inclusion on the register is no longer necessary to prevent fraud) or within 8 years.

Other DPP considerations:

- ***Quality and integrity/accuracy*:** Participating FIs are obliged to correct, remove or supplement data on the external register as necessary to ensure accuracy. Any information entered on the register must be traceable and documented
- ***Transparency/notification*:** The data subject is required to be notified of their inclusion on the register, unless notification would be against the interest of prevention, detection and prosecution of criminal offence or the protection of the data subject.
- ***Fairness in automated decisions*:** While the external register may be queried automatically, each hit must be reviewed at both ends (i.e., both the requesting FI and the FI that entered the data) to ensure it is not a false match. In addition, any subsequent request for information beyond a hit must be considered manually by the Security Department of both the requesting and requested FI.
- ***Data subject's right of access and correction*:** The data subject has the right to inspect, correct, delete and object to data on the register. In most cases, such requests must be responded to within one month with full reasoning. Where such confirmation and access cannot be granted, e.g., if

necessary in the interests of preventing, detecting and prosecuting criminal offences, the internal decision must be recorded.

- ***Data subject's right of redress*:** If there is a dispute about the correctness or legitimacy of registered data, the data subject can approach the board/management of the relevant FI and, if still unresolved, can apply to an external party, such as the Financial Services Complaints Institute, the DPA, or the competent court.
- ***Data transfers/disclosures*:** Data included in the register can only be processed for specific reasons, to prevent and detect fraud, as set out in the IAS operating protocol. Participating FIs each commit to ensure that the data cannot be further processed or used in additional ways or in any way that is incompatible with this purpose.
- ***Confidentiality/data security*:** Only designated authorised officers are able to access the IAS to query the register. Each authorised officer must be subject to a duty of confidentiality. Beyond the initial query (hit/no-hit), any exchange of identifying information takes place exclusively between the Security Department of the participating FIs. Each participating FI commits to maintaining the security of the data and evaluating applicable security measures every two years. FIs must also put in place a procedure for data leaks, consistent with the GDPR.

Additional considerations/challenges:

- ***Financial inclusion***: Inclusion on an FI's internal incident register may coincide with a decision not to offer financial services to the relevant individual or to exit an existing relationship. Authorities are also sensitive to the possibility that inclusion on the external register may lead to similar decisions. To prevent financial exclusion, FIs have committed to continue to provide access to services concerning the basic needs of the individual (e.g., basic bank accounts or basic insurance). In addition, in deciding whether to provide services to a customer, FIs can only take into account information from the IAS after receiving advice from the FI's security department (that manages any data exchange). FIs cannot act solely on the basis of a 'hit' without checking the reason for inclusion.

Involvement of authorities (AML/CFT/CPF or DPP): The project was assessed by the DPA for compliance with DPP requirements, and was approved. The initiative's certification was renewed in 2021. The participating FI's are obligated to re-evaluate the protocol every two years, taking into account relevant developments in DPP regulation and jurisprudence. If re-evaluation warrants an amendment to the protocol, the DPA has to be consulted for renewed approval.

Note: This case study is based solely on available public information. It was not the subject of a focus group with involved parties.
Source: *Incident Alert System Protocol* (2021), available at: *www.verzekeraars.nl/media/9002/protocol-incidentenwaarschuwingssysteem-financi%C3%ABle-instellingen-pifi-2021-eng .pdf*

Box 4.5. Section 314(b) (U.S.): Pre- and post-suspicion private-private sharing to identify and report ML/TF activity

Use case: Legal gateway allowing information sharing between financial institutions, under a safe harbour that offers protections from liability, in order to better identify and report activities that may involve ML or TF.

Intended outcomes/results or achieved results: Section 314(b) of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA PATRIOT Act) allows financial institutions to share information to better identify and report potential ML/TF. In particular, sharing under section 314(b) allows financial institutions to:

- Gather additional information on customers or transactions potentially related to ML/TF, including previously unknown accounts, activities, and/or associated entities or individuals.
- Shed more light on overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.
- Build a more comprehensive and accurate picture of a customer's activities that may involve ML/TF, allowing for more precise decision-making in due diligence and transaction monitoring.
- Alert other participating financial institutions to a customer of whose suspicious activities they may not have been previously aware.
- Facilitate the filing of more comprehensive suspicious activity reports than would otherwise be filed in the absence of 314(b) information sharing.
- Identify and aid in the detection of ML/TF methods and schemes.
- Facilitate efficient suspicious activity reporting decisions, e.g., when a financial institution obtains a more complete picture of activity through the voluntary information sharing process and determines that no SAR is required for transactions that may have initially appeared suspicious.

FinCEN data from the U.S. Financial Crimes Enforcement Network (FinCEN) from 2017-2019 shows that on average 15 900 suspicious activity reports per year reference the use of section 314(b) sharing. Institutions filing reports with reference to section 314(b) had either sent a request to another institution under 314(b) to support their own enquiry into suspicious activity or had received a section 314(b) request that prompted the institution to conduct its own analysis and file a suspicious activity report. Based on data over the 2017-2019 period, there is a trend towards an increasing number of institutions referencing section 314(b) sharing in their reports.

Participants: Engaging in sharing under section 314(b) is voluntary, and open to all financial institutions subject to an AML program requirement under FinCEN regulations, and any association of such financial institutions. Entities wishing to engage in section 314(b) sharing must be registered with FinCEN. As at the end of

2019, there were 7 000 participating institutions. The majority of participating institutions are banks/credit unions, but a range of other sectors are represented, including casinos, securities firms, insurance companies, and money service businesses. All participating institutions are covered by regulations which provide a safe harbour for sharing and require relevant controls which are periodically tested by supervisors.

Mode of information sharing: Section 314(b) allows private-private information sharing under specified controls on the use and security of information. Information may be shared on a one-to-one or a one-to-many basis between organisations registered with FinCEN under 314(b), in writing, verbally, or making use of available technologies. Any organisations sharing under 314(b) must maintain adequate procedures to protect the security and confidentiality of all information shared pursuant to 314(b) and other laws, regulations, and guidelines.

Specific data points collected/shared: Participating financial institutions may share information regarding individuals, entities, organisations, and countries for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering. Section 314(b) and its implementing regulations impose no limitations on the sharing of personally identifiable information, provided such sharing is otherwise consistent with section 314(b) and its implementing regulations. Section 314(b) also does not restrict the type or medium of information that can be shared in reliance, e.g., video surveillance footage or cyber-related data such as IP addresses can be shared, as can verbal or written information. However, section 314(b) does not authorise a participating financial institution to share a suspicious activity report itself or to disclose any information that would reveal the existence of such a report (although institutions sharing information may work together to file a joint report).

Lawful basis for processing personal data: Section 314(b) provides the lawful basis for sharing information. Sharing under section 314(b) is protected by a safe harbour that offers protection from liability for sharing consistent with section 314(b) and its implementing regulations. Section 314(b) sharing is appropriate when the financial institution or association of financial institutions has a reasonable basis to believe 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.

Assessment of proportionality: In order to share information under section 314(b), the sharing institution must have a reasonable basis to believe that the information relates to activities (e.g., fraudulent transactions or cyber events) that may ultimately be related to ML/TF. Section 314(b) implicitly demonstrates that information sharing within the 314(b) parameters is reasonable to fulfil the purposes of the sharing, i.e., the sharing is proportionate in relation to the purposes of the sharing—detection of potential activity that may ultimately be related to ML/TF and protecting the public from financial crime and terrorism.

Other DPP considerations:

- ***Data transfers/disclosures*:** Data shared pursuant to Section 314(b) may only be used for the purposes laid out in the section and its implementing regulations, i.e., identifying and, where appropriate, reporting activities

that may involve ML/TF; determining whether to establish or maintain an account or to engage in a transaction; or assisting in compliance with AML requirements.

- ***Data quality and integrity:*** Financial institutions utilising 314(b) may improve the accuracy and integrity of their information, including information that may need to be reported to FinCEN in a suspicious activity report.
- ***Fairness in automated decisions:*** Financial institutions utilising 314(b) are engaging in information sharing, with human oversight, specifically to improve the accuracy and integrity of their information, including information that may need to be reported to FinCEN in a suspicious activity report, which helps ensure fairness to individuals involved in those activities.
- ***Confidentiality/data security*****:** Financial institutions must establish and maintain adequate procedures to protect the security and confidentiality of all information shared pursuant to section 314(b). This includes designating a point of contact for receiving and providing information. Prior to sharing information, financial institutions must take reasonable steps to verify that the receiving institution is registered to participate in section 314(b) sharing. FinCEN provides access to a list of participants that registered financial institutions and associations of financial institutions can use for this purpose.

Involvement of authorities (AML/CFT/CPF or DPP): Financial institutions that wish to use section 314(b) to share information are required to register with FinCEN and to update their registration on an annual basis. Government agencies, including FinCEN, are not involved with and do not see any specific information shared amongst financial institutions using the 314(b) safe harbour unless such information sharing is referenced in a suspicious activity report.

Source: Discussions with and input from participants in s.314(b) sharing, U.S. Treasury, Section 314(b) Fact Sheet, available at: *www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf*; U.S. Treasury, Information Sharing Insights: Section 314(b) Participation and Reporting, available at: *www.fincen.gov/sites/default/files/shared/314bparticipationinfo.pdf*

Box 4.6. AML Bridge (Estonia): post-suspicion private-private information sharing initiative

Use case: AML Bridge is a secure digital platform provided by an independent 3rd party company. It allows member banks to exchange pseudonymised data (largely transaction data) with one or more other banks in an end to end encrypted format. The list of receiving institutions is defined individually by each member for each exchange. Information is shared on a near-to real-time basis to pursue collaborative investigations.

Intended outcomes/results or achieved results:

- As of March 2022, AML Bridge has seen 1200 private-private 'collaborative investigations' completed since it was established in July 2021 (~150 cases per month).
- Half of these cases (over 600) involved ML investigations, which has increased the quality of STRs submitted, including by promoting joint STRs. These cases have also helped to clear non-suspicious customers more quickly (i.e., reduce false positives).
- One third of the cases (over 400) relate to 'scam fraud', which generally means a form of authorised push payment (APP) fraud.[1] Approximately EUR 3 million has been recovered from criminals and returned to victims with the help of AML Bridge. For fraud, speed is key and AML Bridge enables most of the urgent cases to be resolved in under 15 minutes.
- Collaborative investigations related to sanctions evasions were initially a small category. However, following Russia's invasion of Ukraine (in March 2022) these cases account for the majority of AML Bridge usage, with weekly volumes quadrupling over the course of March 2022. The dominant use case is quickly clearing new exact-match false positives, which are overwhelming sanctions teams and frustrating good customers. In addition, the network is observing opportunities to start sharing and spreading information about close associates and owned companies of sanctioned persons and entities.

Participants: The AML Bridge platform is provided by an independent 3rd party company (a 'data processor' under the GDPR). AML Bridge was first launched between four of Estonia's largest banks (collectively representing 90% of transactions) and has since expanded to include all 10 Estonian banks and several non-banks in the country. A range of individuals and teams within the banks play critical roles in the project, including ***CEOs*** (executive support), ***MLROs*** (Steering Committee members), ***Data Protection Officers*** (advisors), ***information security teams*** (to ensure a secure platform for sharing). In addition, each bank appoints ***project leads*** who attend the Steering Committee, act as the first point of contact between the platform provider/data processor and the bank, and co-ordinate internally. The end-users of the AML Bridge are the bank ***'crime fighting' teams*** (AML/CFT/CPF, sanctions screening, transaction monitoring, anti-fraud, etc.) who run the operational work and provide constant feedback on the platform.

Specific data points collected/shared: The data shared is mostly transaction data and is shared on a near-to real-time basis. The exact structure of shared data is configurable and determined based on the suspected offence and the individual network members. Sharing using "scenario templates" allows participants to define the input fields required for the recipient in order to identify the subject (e.g., customer name, account number, transaction ID) and the requested specific data (e.g., full name, date of birth, source of wealth, payment reason, risk level, potential red flags, copies of the documents, etc.). Data-sharing covers

investigations/enquiries around potential ML, sanctions evasion, fraud and related incidents.

Lawful basis for processing personal data: As the controllers of the data, each bank must have a legal basis to share data through the AML Bridge platform. In most cases, the banks will share and process information on one of two grounds under the GDPR: 'compliance with the law' or 'legitimate interest' (GDPR, Article 6.1(e)). In addition, Estonia's ML/TF Prevention Act establishes some limitations of DPP rights of data subjects on the basis that AML/CFT/CPF activities are classified as a matter of public interest. In particular, the Act states that financial institutions are allowed to share personal data for collaboration purposes (section 16) and that, in such cases, certain privacy rights of the data subject can be restricted based on the public interest of AML/CFT/CPF activities (section 48). Each participating bank signs a Data Processing Addendum (a contract between the bank and the platform provider/data processor to protect data in compliance with the GDPR).

Assessment of proportionality: The extent and amount of data shared, its geographical scope and its retention periods are defined by the banks using the platform. Nevertheless, the design of AML Bridge limits the amount and type of data being shared to help institutions minimise sharing; the platform has extensive audit logging to help banks conduct reviews and quality assurance checks and identify unreasonable actions.

Other DPP considerations:

- ***Transparency/notification and rights of data subjects***: The Data Processing Addendums stipulate that the platform provider/data processor will provide all reasonable assistance to the data controller (the bank) for the fulfilment of the controller's obligation to respond to requests from data subjects exercising their data protection rights. If any such requests are received by the platform provider/data processor, they are forwarded to the bank with all relevant information.
- ***Confidentiality/data security:*** The AML Bridge has an information security management system in place which includes strict access control (including Multi-Factor Authentication and IP whitelisting), encryption (in transit and at rest), disaster recovery (with backups and regular testing) and audit logs. Security documentation, including audit reports, is available to all participants. The security of the platform is tested at least annually by a qualified third party and all participating institutions have the rights to do their own penetration testing (one bank has used this right and shared the results with other participants).

Technologies utilised: AML Bridge uses end to end password-based encryption. All messages are encrypted with a private plus public key pair, and in order to decrypt messages, the user has to gain access to their private key by entering another password, which is different from their main login password. Neither the platform provider nor any other party has access to this key.

Additional considerations/challenges:

- ***Unclear regulations are the biggest barrier to private-to-private data sharing:*** Banks were only willing to start sharing information in a way that was explicitly permitted under the relevant legislation and regulations.
- ***The GDPR is not a barrier, but an enabler of financial crime data sharing:*** The consistent framework across private banks and regulators allows all participants and entities involved to quickly agree whether a particular form of private-to-private financial crime data sharing is acceptable.
- ***Regulators (especially supervisors and data protection authorities) must be involved from the beginning:*** The success of AML Bridge comes, in part, from its governance. Regulators are often adversarial with those they are regulating; this project avoided major setbacks by keeping all stakeholders not only informed but actively involved. Banks gained confidence to innovate because there was no risk of a negative surprise from the FSA or DPA.
- ***Within banks, executive sponsorship is a necessary precondition to kick off new data sharing initiatives:*** It takes significant effort from a variety of teams and individuals, across many months, to create and implement a financial crime data-sharing initiative. It has to be a priority from senior bank leadership.

Involvement of authorities (AML/CFT/CPF or DPP): Government oversight of AML Bridge is provided by the ***Financial Supervision Authority*** (which is a member and observer of the AML Bridge Steering Committee), the ***FIU*** (Steering Committee member), and the ***Data Protection Authority*** (Steering Committee observer).

Source: Discussions with and input from AML Bridge participants, *AML Bridge*, available at: *https://salv.com/uploads/AML-Bridge-Estonia.pdf*

Note:

1. APP fraud is where an individual is deceived into sending a payment to a bank account controlled by the fraudster. Often, this occurs by the fraudster obtaining information on the victim (e.g., via access to a hacked email account) and impersonating a legitimate company with which the victim is doing business. APP fraud may also include investment or romance scams. As the victim authorises the payment, it is often difficult or impossible to reverse/revoke the transaction.

Box 4.7.safeFBDC (Safe Financial Big Data Cluster) Prototype (Germany): early stage project for private-private information sharing initiative

Use case/purpose of the initiative: The safeFBDC (safe Financial Big Data Cluster) prototype project is part of the European GAIA-X initiative, which aims to create a unified ecosystem of cloud and data services protected by European data laws. It is a platform on which AI applications for the European financial sector are developed and made available. The financial data platform enables a secure exchange of data while maintaining individual data sovereignty. In the AML use

case, financial data from banks are brought together on the safeFBDC platform and applications are set up to combat money laundering.

Intended outcomes/results or achieved results: Financial data pooling from across the industry to significantly improve the performance of AI algorithms, driving efficiency and transparency. For example, the AML use case realises a graph network approach to identify money laundering activity.

Participants: A German company (Deutsche Börse Group) is responsible for the workstream, alongside three technology providers (Spotixx, HAWK:AI and Google), four financial institutions (Commerzbank, Deutsche Bank, Helaba and ING), and the Hessian Ministry of Economics, Energy, Transport and Housing (a state authority).

Mode of information sharing: A decentralised ecosystem allows data to be stored in federated silos owned by the banks and only pooled in a closed environment for the duration of the runtime of the algorithm. The pooled data is deleted right after processing is finished.

Specific data points relevant for the initiative: Initially, SEPA transactions will be used. Suitable requirements for a minimal viable dataset have been formalised with specific attention to the trade-off between censoring of end-client level information and required algorithm learning performance.

Use of privacy enhancing or other technologies: Data is encrypted at rest and in transit. Static decentralised tokenisation of the personal identifiable data ensures safety even in the event of a leak. Additionally, the prototype infrastructure does not allow any user to directly interact with the data. Only algorithms which have been pre-approved by the data owners can access the data.

Legal basis: As an early stage project, where data is not yet being transferred, participants are still in the process of identifying the most appropriate legal basis for sharing. Data owners must preapprove algorithms that can run on the data. Hence, the data owner is in full control of which data is processed and in which manner and how the results are handled. Personal data is transferred, although it is not shared with other entities because of a tokenisation approach and the design of the closed data pool. In addition, specific regulations form a more general legal basis, for example the requirement to preform AML monitoring and to report suspicious transactions.

Assessment of proportionality: The initiative works with a minimal viable dataset assumption, focusing on creating a no trust environment. When the data is transferred, it leaves the control of the data owner only for the time of calculation into a secure and closed space and is deleted right after calculations.

Other DPP considerations:

- ***Quality and integrity/accuracy*:** Transaction data accuracy and completeness are ensured because banks provide data directly to the platform. Emphasis is further put on high standards on data validation and testing, including back-testing, of algorithms. Overall, this also ensures the integrity of the output data.

- ***Transparency/notification*:** AML monitoring and reporting are deeply embedded in a bank's workflow, meaning that established systems can and will be used as core pillars in the new approach.
- ***Fairness in automated decisions*:** The algorithms report suspicious patterns which is then subject to further comprehensive investigation.
- ***Data transfers/disclosures*:** The output of the algorithm is controlled by the data owner, and prevents sensitive information being disclosed. Alerts are generated on the back of suspicious patterns detected by the model. Otherwise, disclosure and data transfer practices remain unchanged.
- ***Confidentiality/data security:*** Personal data does not leave the data space of the data owner without being pseudonymised. All security standards for encryption are followed and key management can be handled by each respective data owner. Any change to the access authorisation is logged and can be validated. Algorithms can only be executed by the system upon the a digital signature of each data owner.

Source: Discussions with and input from relevant authorities in Germany.

Box 4.8. EuroDaT (Germany): early stage framework for information sharing

Use case/purpose of the initiative: EuroDaT is a project funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK). It aims to build a European data trustee that enables data sharing, with a focus on financial data, in a manner compliant with GAIA-X (a project working towards a European federation of data infrastructure and service providers and European digital sovereignty). One of the envisaged use cases is fraud detection.

Intended outcomes/results or achieved results: The trustee aims to facilitate semi- or fully-autonomous sharing while remaining DPP-compliant and maintaining a low barrier of entry for participants.

Participants: The project seeks to vary participants depending on the use case, but they include a state ministry (Ministry of Economics, Energy, Transport and Housing, State of Hessen), academics (ZEVEDI, University of Saarland, Goethe University Frankfurt, DFKI), and technology providers (ATOS, Deloitte, d-fine. Lexemo).

Mode of information sharing: EuroDaT explicitly does not want data to be pooled or centrally stored. Instead, EuroDaT intends to act as an information platform through which data can be piped for individual queries. This concept of data transactions is vital: the trustee does not act as a repository of data for interested parties to draw from. Instead, individual data providers and data users are connected. According to contractual or other legal connections between the parties, data is transmitted for each individual process. The data is stored temporarily in flash vaults within the trustee that are inaccessible even to the trustee itself. Therein, the data can be analysed by algorithms provided by either

data giver, data receiver or a third party. The trustee passes on the results to such parties as is agreed. Afterwards, it erases the data permanently.

Specific data points relevant for the initiative: There is currently neither a limit nor proscription on the types of data or the specific data points that can or will be shared through EuroDaT.

Legal basis: As an early stage framework, where data is not yet being transferred, participants are still in the process of identifying the most appropriate legal basis for sharing. The flexibility of the EuroDaT Project means that each data transaction must be analysed on its own terms and different types of data fall under different DPP regimes and bases for sharing.

Assessment of proportionality: EuroDaT will establish an infrastructure for data analysis and does not decide on data processing itself. The responsibility for DPP concerns lies primarily with the clients, who make the decision on data processing. EuroDaT plans to offer a data taxonomy to make categorising different data easier and thereby help to identify and avoid data protection risks.

Addressing DPP considerations:

- ***Quality and integrity/accuracy*:** The responsibility for maintaining the data for accuracy and completeness therefore lies with the providing parties. Depending on the specific use case, it may be necessary to develop common standards.
- ***Transparency/notification*:** The current AML use case plans to build on existing systems and enable better cooperation between banks without requiring disclosure of data. Current models on transparency/notification should therefore be transferable.
- ***Data transfers/disclosures*:** Currently, the project envisions clients maintaining full control over their individual data. This means that further transfer or disclosure of any data shall be both contractually prohibited but ideally also technically impossible, since the trustee shall have no access to the actual data sets.
- ***Confidentiality/data security:*** The trustee is founded on the idea that data can only be processed in such a way as is determined ahead of time by the data giver. The trustee ensures a perfectly safe and anonymous environment that guarantees data will not be accessed by unauthorized third parties. The trustee also maintains logs, both of contractual agreements made between parties as well as the access granted to different parties based on such agreements. This also means that the trustee cannot guarantee that data is processed lawfully. In order to do that it would need to possess identifying information about the data. This runs counter to the principal idea of a trustee.

Discussion of other considerations/challenges and any lessons learnt: Fundamentally, the trustee cannot take the burden of considering DPP principles away from its users. The responsible party (i.e., the financial institutions) will always have to ensure that they possess and process data in a legal manner. This is proving a challenge. Most interested third parties (including financial institutions) are looking for the trustee to address DPP requirements. While the

trustee hopes to make data transactions and the associated DPP considerations more streamlined, it is not yet at such a state. Instead, working with the trustee, especially at this early stage, is still considerable work for third parties, including the financial sector. Data controllers are in the best position to describe and understand their own DPP considerations and the principles as they apply to them. This needs to be translated into the creation of the trustee and the attendant functions. Only by working together as closely as possible can the trustee and interested third parties hope to standardise and automate future taxonomies of data and their processing.

Source: Discussions with and input from relevant authorities in Germany.

SECTION FIVE:
What are the potential issues that arise in implementing private sector information sharing for AML/CFT/CPF in line with DPP frameworks and requirements?[33]

29. This section sets out some common issues that arise in designing and implementing private sector information sharing for AML/CFT/CPF purposes, based on the feedback received from focus group discussion on the case studies above, feedback from public authorities, and industry engagement.[34] The next section (Section 6) contains recommendations for the public and private sector that may help to address these issues. The FATF hopes that this work will assist countries that are considering embarking on private sector information sharing mechanisms to understand how their peers have addressed DPP obligations in designing information sharing initiatives. However, each potential initiative needs to be considered on a case-by-case basis depending on their unique characteristics and the relevant DPP requirements.

Policy issues

30. The case studies covered in the previous section indicate that the involvement and engagement of public authorities appears to be a significant factor in the success of private-sector AML/CFT/CPF information sharing initiatives. Authorities can play different roles with varying degrees of involvement[35] based on the objectives of the

33 Section 6 of the Phase 1 Stocktake Report provides an overview of the challenges related to the use of new technologies for data collaborative analytics.

34 During the period from October 2021 to June 2022, the FATF project team has conducted six focus group discussions and presentations with jurisdictions including Estonia, Germany, the Netherlands, Singapore, the United Kingdom and the United States. Other engagement and discussions with public and private sector stakeholders in Europe by the Secretariat have also been held.

35 For example, both AML/CFT and DPP authorities in the UK are joined up in supporting the private sector as projects develop and, in the case studies above, the ICO was involved in the sandbox, which allowed the data processor to address data protection challenges before they developed products and services. The financial supervisor in Singapore has taken a leading role in bringing together different private and public sector stakeholders in organising and shaping the sharing initiative. The Ministry of Finance (also responsible for AML/CFT issues) in the Netherlands has taken into account the proposal submitted by private sector and incorporated the elements of sharing initiative in their revised and upcoming national AML/CFT strategy.

sharing initiatives and the authority's willingness to provide guidance (at least at a high level) to institutions they supervise. Nonetheless, a total **absence of government engagement, especially in the early stages,** has often increased the challenges to private sector information exchange.

31. In the absence of a clear contact point or leading agency in spearheading sharing initiatives, the information shared between private sector institutions **may not necessarily align with national AML/CFT/CPF objectives and priorities**. As seen in some of the use cases (e.g., the COSMIC project; Box 4.2), the participation of a few selected or interested financial institutions in the sharing initiatives, instead of all of them, has the potential to lead to risk migration, i.e., criminals may shift their transactions to non-participating financial institutions.

32. In addition, successful information sharing can be hampered by a lack of engagement between AML/CFT/CPF and DPP authorities, or the **absence of a communication or co-ordination mechanism between AML/CFT/CPF and DPP authorities.** Such engagement is important to provide assurance/clarity in information sharing, and to improve the development of sharing initiatives. A lack of engagement between these authorities can result in conflicts based on a lack of mutual understanding of the critical public interests involved in both protecting the public from crime and terrorism and protecting privacy and personal data.

33. Participants in the information sharing projects described in the case studies above (see Section 4) also highlighted that without government support, private sector entities have experienced **difficulties gaining the support of peers and feedback from DPP authorities**. Such support and feedback is necessary to explain the utility of sharing initiatives (e.g., improving the quality of STRs) and to illustrate how and why private sector information sharing would meet wider public interests (including serving AML/CFT/CPF objectives; reducing low quality or false positive/negative STRs that do not protect the interests of legitimate customers/transactions; or preventing de-risking).[36]

34. As noted and illustrated in the case studies above, **there has yet to be a "model template" of private sector information sharing** that may comply with and advance both AML/CFT/CPF and DPP requirements. As set out in Section 3, data protection legislation is largely principles-based, meaning that implementation is context-dependent and involves balancing competing policy objectives. DPP authorities will therefore have to consider each sharing proposal on a case-by-case basis. They may not be comfortable endorsing a specific project or approach, given the risk that their endorsement is perceived as confirming the project has met all DPP requirements. An absence of co-ordination and collaboration between AML/CFT/CPF and DPP authorities can result in limited understanding of the relevant policy objectives. As a result, DPP authorities are unlikely to provide the guidance that financial institutions need to invest in and move forward with an initiative.

---

[36] De-risking is the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach (see FATF, "FATF clarifies risk-based approach: case-by-case, not wholesale de-risking", available at: https://www.fatf-gafi.org/documents/news/rba-and-de-risking.html). E.g., Additional information may help clear suspicions in certain cases and as a result allow a fair access to financial services.

35. Section 6 includes a range of recommendations to address these issues, including active facilitation by the public sector (para.51-52), regular dialogue between DPP and AML/CFT/CPF authorities (para.53-55), and early and ongoing engagement between the private sector and DPP authorities (para.60).

Legal issues

36. The range of national and international DPP laws and regulations has also posed challenges for private-to-private information sharing projects. Interested financial institutions have devoted substantial effort to reviewing laws, regulation and other supervisory/regulatory instruments (including the international laws and multilateral frameworks set out in Section 3) to ascertain the legality of such sharing arrangements within each specific jurisdiction. There are a wide range of legal requirements and principles that institutions may have to consider (see Section 3). By way of example, some of the particular challenges raised by participants in the initiatives described in the case studies include:

- **Is sharing information for AML/CFT/CPF purposes with other financial institutions or across borders between entities within the same group (in addition to supervisors or operational agencies) lawful, compliant with, and permitted under AML/CFT/CPF and DPP rules? Is it in line with any contractual arrangements with customers concerning data rights/use?** As a first step, institutions need to determine whether information proposed to be shared qualifies as personal or non-personal information under the relevant legal framework(s), and therefore whether relevant DPP rules apply. DPP rules often require the sharing of data to be 'necessary' or 'proportionate', to achieve 'legitimate interest', and/or to be explicitly permitted in legislation (in addition to a range of other possible requirements; see Section 3 above). Some participants in the initiatives mentioned above (see Section 4) noted the challenge of demonstrating that sharing was 'necessary' prior to testing a sharing initiative to obtain clear and definitive results. Private sector entities may be unwilling to take the legal risk in developing initiatives in the face of any perceived legal uncertainty posed by DPP laws, or where they do not have any input from the relevant leading/co-ordinating government policy departments, or where the initiative is not required for STR reporting by national governments (or in the relevant FATF Standards). The latter is particularly common for data shared prior to the forming of a suspicion in light of the stricter requirements that often apply to such sharing.
- **Is the sharing of customer/transaction data based on collaborative analytics and automated analysis fair, necessary and proportional, and would it infringe the legitimate interests and rights of customers (in jurisdictions with these standards)?** Pre-suspicion sharing of personal information is often subject to much stricter limitations because it applies to a broad set of data. In some jurisdictions, sharing information at this stage may not be permitted under the DPP laws. Institutions in certain jurisdictions may therefore need to carefully consider mechanisms to eliminate any personal data shared at the pre-suspicion stage (e.g., the use of PETs or adjustments in data scope; see Section 6). As to post-suspicion information sharing, some financial institutions may seek further guidance on how to use information obtained from an information sharing initiative in functions other than for reporting STRs – for example, whether the information can be used for updating customer due

diligence information, risk assessment and management, or termination of the customer relationship, and whether these secondary uses would be considered fair,/legitimate/necessary/proportionate/compatible with the original purpose of detecting suspicious activity.

- **In jurisdictions and situations where consent may be relied upon as a lawful basis for sharing, is sharing compliant with existing consent obtained from customers?** Relying on consent assumes that the financial institution has met the usual DPP requirements for transparency in its privacy policies, customer notices, and other statements available to customers, e.g. by providing information on the types of third parties that would have access to the personal data and how it is being processed. While general consent to meet the usual DPP requirements would often have been previously obtained from customers for onward sharing for AML/CFT/CPF or other crime prevention/detection purposes, such notice of sharing typically has focused on sharing with operational agencies such as FIUs or law enforcement agencies, but not other financial institutions. Changing consent provisions to accommodate new data sharing practices also presents logistical challenges (e.g., for existing services and customers) and a subsequent withdrawal of consent would also prove problematic (in terms of compliance with DPP principles: see Section 3, para.22). Relying on consent may also be problematic in some jurisdictions in situations where the consent could be construed as being coerced or not freely given, for example, if the customer has no other option to receive the specific financial services involved or where consent is demanded as a condition of service. For these reasons, consent is unlikely to be the most viable, or the sole, lawful basis for AML/CFT/CPF related sharing.
- **Do information sharing initiatives risk breaching tipping-off provisions and prohibitions against disclosing STRs?** As highlighted in Phase 1 of this work (see section 6.5 of the Phase 1 Stocktake Report), institutions involved in sharing initiatives would need to devise additional measures to ensure that any sharing of customer/transaction data, and the possibility of resulting adjustments in customer relationships or risk rating, will not lead to tipping-off or go against the relevant FATF Standards (e.g. Recommendation 21). Some participants in the initiatives described above (see Section 4) encountered confusion as to whether any information sharing with a third party (not the client itself) could constitute tipping off. At times, the private sector finds it challenging to devise the right set of measures that would satisfy both the objectives of information sharing and confidentiality/tipping-off, without relevant guidance from supervisors/regulators. Future initiatives could also consider designing platforms in a manner that prevents tipping off (e.g., using encrypted queries on decentralised data).

37. In some cases, while the use of data may be relevant to criminal investigations, such uses can limit the ability of participating financial institutions to be transparent with the data subject and provide the avenues for redress required by DPP rules. FATF's rules to prevent tipping-off (Recommendation 21) support the objective of safeguarding the confidentiality of criminal investigations and are required to be set out in domestic law or regulation. The FATF Standards (Recommendation 2) also require co-operation and co-ordination to ensure compatibility of AML/CFT requirements with DPP rules. Depending on domestic DPP laws, exceptions and exemptions to privacy rights for purposes of prevention, investigation, detection or

prosecution of crime may apply. The case studies highlight the need for agreed safeguards (e.g. the requirement for financial institutions using alerts from an AML facility to undertake its own investigation) and possibilities for data subjects to appeal decisions to remove access to financial services and provide clarifying or additional information.

38. Section 6 includes a range of recommendations to address these issues, including active facilitation by the public sector (para.51-52), pursuing data protection by design (para.58-59), early and ongoing engagement between the private sector and DPP authorities (para.60), and developing indicators and metrics to measure success (para.61).

Operational issues

39. Some of the challenges identified in previous FATF's work (e.g. the Phase 1 Stocktake Report) remain valid in recent private sector information sharing initiatives. These challenges are relevant to both public and private sector entities involved in sharing initiatives. The private sector can face these challenges at institution or at sector level. The recommendations in Section 6 aim to share lessons learned in the case studies to help other jurisdictions navigate these challenges. They also aim to ensure that the private sector information sharing initiatives are effective, efficient, and timely, and avoid delaying the detection of potential suspicious transactions or customers/criminal network, while complying with relevant DPP requirements.

40. **Data scope:** Some of the case studies highlighted challenges in determining the scope of data shared, while achieving the aims of the initiative. In order to comply with DPP requirements (e.g. lawfulness of data sharing and minimising the data to only what is necessary to achieve the specific purpose of the project), some of the sharing initiatives have adjusted and reduced the scope and types of data shared. This challenge is particularly relevant for pre-suspicion sharing; to align with the relevant DPP rules and minimise (or eliminate) the scale and involvement of personal data, some projects have focused on particular types of data (e.g., transactions by legal persons) which generally contain less or no personally identifiable data. Other projects have reduced the number of data points shared to ensure the data shared is only the data necessary for the initiative. As a result, some of these sharing initiatives faced challenges meeting their original goals and consequently had to review and revise their initial sharing objectives and adjust their expected sharing outcomes. While narrowing the scope and data used in the initiative helps ensure compliance with DPP rules, feedback from some private sector participants in these sharing initiatives has indicated that this can also reduce or undermine the utility of the project. Additionally, it may raise questions as to whether the data shared would be sufficient to meaningfully aid participating private sector institutions in understanding the suspicious transactions that take place across different institutions.

41. **Data accuracy and reliability:** Some case studies have made use of privacy enhancing technologies (PETs) to mask the personal identity of customers, as part of the process of safeguarding data privacy. Some participating private sector entities noted that PETscan pose operational challenges depending on how they are used. For example, in some projects, the specific PETs used may not have been fit-for-purpose, making it more difficult to determine the accuracy of the data

received/shared, thereby affecting the reliability and quality of sharing. In addition, project participants had to spend additional resources to trace back the identity of the relevant shared data before conducting any further meaningful follow-up such as monitoring or filing an STR. These challenges can be magnified where there are also issues in data preparation and interoperability. Challenges can also arise where records cannot be effectively linked, creating a risk of ambiguous record linkage (i.e., that information or data relating to two unconnected is erroneously linked).

42. **Data security**: Generally speaking (regardless of whether PETs are used or not), private sector participants would need to devise a secured sharing channel among participants. This is a fundamental step as any leakage of data stored and communicated as part of the sharing initiative could have serious consequences, including on customers' data rights, AML/CFT/CPF effectiveness, public trust in the data sharing initiative and institutions involved, and financial and non-financial harm for individuals involved.

43. **Data and system readiness**: As in any data transformation and information sharing initiatives, the absence of structured data and differences in data format and classification, leading to a lack of interoperability, have all slowed down the launch of some sharing initiatives covered in the previous section. A number of projects have taken three to five years to clean and match data before the data is ready for sharing or analysis purposes. Inadequate IT capacity has prolonged the formal implementation of sharing projects on other occasions, as participating private sector institutions would have to upgrade their IT tools (as well as staff IT skills) to allow sharing. As such, interested private sector entities should consider and plan ahead data interoperability projects to facilitate a successful launch of sharing initiatives.

44. Section 6 includes a range of recommendations to address these issues, including pursuing data protection by design (para.58-59), applying PETs (para.56), and taking steps towards data preparation (para.57).

Other issues

45. **Provision of financial services to affected customers/De-risking**: Private sector information sharing initiatives may help participating institutions identify certain customers or transactions for further monitoring in accordance with their AML/CFT/CPF requirements and their usual internal policies and procedures for investigating possible criminal financial activities and taking action as warranted. These initiatives could reduce the number of false positive STRs, reducing the impact on customs and government authorities. As with any findings of problematic activities based on the investigation of specific transactions, this may eventually lead to exiting customer relationships or excluding the provision of certain financial services to certain individuals to manage risk. As set out in the Phase 1 Stocktake Report, *"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."[37]

46. It is important to note that, even in the absence of private sector information sharing, de-risking can occur and the additional concern here is the potential for multiple effects or over-reliance on information sharing initiatives. The opposite argument also applies, that information sharing may increase the accuracy and reliability of information, thereby improving risk understanding and decision-making reliant on that data, and reducing de-risking.[38]

47. **Competition**: As set out in the Phase 1 Stocktake Report, "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. 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." The initiatives should be limited to the sharing or accessing of data that is required for AML/CFT/CPF purposes.

48. **Cross-border sharing**: As seen from the case examples, DPP rules applicable in a jurisdiction/region will affect the form and scope of a private sector sharing initiative in that location, including the type of data allowed to be shared, the purpose for which it can be shared, and the specific legal grounds for sharing. As a result, the sharing initiatives implemented to-date, despite extensive resources allocated, are seldom replicable or able to be scaled-up in other jurisdictions. In turn, this limits the value of the sharing initiatives as it often restricts the project to a single jurisdiction only, thereby making it difficult to be expanded to a cross-border sharing initiative to identify cross-border suspicious activities or networks. For example, this may prevent such initiatives from helping to identify more complex ML using correspondent banking networks or through trade finance. In general, the institutions that are involved in these initiatives are large international or regional banks that obtain data from several jurisdictions within their financial group. The involvement in private sector information sharing platforms in one jurisdiction may raise compliance concerns for another part of the institution if operating under different DPP standards (or different interpretations of standards).

---

37 FATF Phase 1 Stocktake Report, paragraph 89.

38 The Financial Stability Institute noted that improved information sharing could help to reduce unwarranted de-risking, thereby supporting financial inclusion: Financial Stability Institute (September 2020) *Closing the loop: AML/CFT supervision of correspondent banking*, available at: www.bis.org/fsi/publ/insights28.pdf

49. Section 6 includes a range of recommendations to address these issues, including adopting measures to prevent de-risking (para.62) and active facilitation by the public sector (para.51-52).

SECTION SIX:
What are the key recommendations for effectively implementing a private sector information-sharing initiative for AML/CFT/CPF purposes while complying with DPP rules?

50. While navigating the challenges described in the previous section can be daunting, information sharing initiatives in both established and pilot phases have achieved progress. Based on focus group discussion on the case studies, some of the overarching recommendations for successful information sharing and collaborative analytics that promote AML/CFT/CPF effectiveness are:

    1. To prepare a data protection impact assessment (DPIA) to clearly define the purpose and objectives of the information sharing, the data to be processed and why such data is necessary and reasonable/proportional to achieve the stated purpose, and the legal basis and safeguards to be applied.
    2. To engage with applicable DPP authorities from the beginning of the sharing project, at the design stage. Noting that DPP authorities may not always have adequate resources to engage with individual organisations, general engagement and outreach could occur through a sector-wide or industry group-led approach. This may also help communicate lessons more quickly to the relevant sectors, and ensure any lessons learned are not treated as proprietary information by the institutions involved.
    3. To consider safeguards to adequately protect customer data, including PET and anonymisation/pseudonymisation[39] where useful.

51. There is no one-size-fits-all solution that addresses all AML/CFT/CPF and DPP objectives for all financial institutions globally. The information sharing initiatives explored under this project and in the Phase 1 Stocktake Report have different objectives, DPP legal requirements, technologies and modes of operation and therefore rely on different legal bases and apply various mitigation measures to

[39] Noting that the DPP requirements will differ depending on the extent of anonymisation. E.g., Under the GDPR, anonymous data (i.e., data with no personal reference and that cannot be related to a person) is not subject to the GDPR requirements, unlike pseudonymised data.

achieve AML/CFT/CPF and DPP objectives. A key element is to involve a range of stakeholders, take into account local regulation and context, take a phased approach and build public trust and understanding in developing solutions. The recommendations below are in addition to the Suggested Actions to Support the Use of New Technologies for AML/CFT identified in the first phase of the project. They apply to public and private sector entities interested in developing private sector information sharing initiatives.

Recommendations relevant to the public sector:

Public sector should consider taking an active facilitation role

52. Based on findings of various focus group discussions, having the national AML/CFT/CPF co-ordinating agency, a supervisor or an FIU, take an active role in spearheading information sharing initiatives generally helps private sector institutions overcome a number of challenges, particularly legal challenges. This may also facilitate the engagement of other relevant public authorities, particularly the DPP authorities, or agencies on consumer protection and competition.[40] The involvement of public authorities can also facilitate co-ordination with international counterparts, to test how and whether cross-border sharing initiatives could be pursued in compliance with DPP requirements. Convergence in the DPP regimes of different jurisdictions, for example due to efforts in multilateral fora (see Section 3), can facilitate the design of cross-border initiatives that respect DPP rules and obligations, but active government engagement in these efforts is vital.

53. While in no way a requirement under the current FATF Standards, authorities interested in facilitating private sector information sharing to promote AML/CFT/CPF effectiveness (whether they are AML/CFT/CPF competent authorities or not) could, for example:

- **Consider updating existing legal or supervisory instruments, either to permit sharing or to provide an exception/exemption to restrictions on sharing**. This applies to those jurisdictions that do not have specific legislation or supervisory instruments specifying the lawfulness of private sector information sharing for AML/CFT/CPF purposes. Such primary legislation provides the strongest legal basis to allow data sharing and processing for AML/CFT/CPF purposes, while providing the necessary safeguards in terms of DPP. This legislation could consider the role of both AML/CFT/CPF and DPP authorities in relation to information sharing initiatives. For example, the IAS case study (Section 4, Box 4.4) shows the specific role of the DPP authority in regularly certifying the sharing initiative in the Netherlands. Primary legislation and a clear role for the DPP authority would help ease private sectors' business and legal concerns in initiating/implementing sharing initiatives. For example, in Singapore, the financial sector supervisor (MAS) has prepared the draft regulatory and legislative framework for the sharing of information between

[40] Based on focus group discussion on use cases, government agencies such as financial supervisor, FIU, DPP authorities, as well as policy departments on finance, security or justice are generally involved in the engagement and discussion with the sharing project proponent data controller, and often, the data processor. In some cases, other government agencies such as those on fraud investigation, digital innovation, competition, consumer protection are also involved in the discussion.

financial institutions for AML/CFT/CPF purposes under COSMIC (Section 4, Box 4.2). The MAS has also made efforts to conduct relevant public consultations prior to the launch of the proposed legislation. Similarly, the Ministry of Finance of the Netherlands has taken the initiative to introduce a legislative amendment to enable full-scale collective transaction monitoring as part of the sharing initiative of TMNL (Section 4, Box 4.3). The 314b case study in the U.S. (Section 4, Box 4.5) also demonstrates the utility of primary legislation.

- **Make use of regulatory sandboxes, pilot programmes or other mechanisms to test information-sharing initiatives (particularly those involving new technologies) in a controlled manner**. Regulatory sandboxes provide a mechanism through which firms (e.g., financial institutions or technology providers) can test data-sharing innovations and conduct live experiments under a regulator's supervision. This allows authorities to understand the implications of different policy choices, and build trust in the use of data-sharing initiatives. In addition, a sandbox environment can help an intiative obtain data or other information to clearly assess and demonstrate the necessity and proportionality of the sharing. Given the intersection between various regulatory frameworks, **joint sandboxes provide a particularly useful platform for testing AML/CFT/CPF data sharing initiatives** (e.g., with the involvement and support of AML, DPP and competition authorities).

- Similarly, pilot programmes provide an opportunity for initial, more limited sharing to measure anticipated benefits and assess whether expansion is necessary. The TriBank pilot (Section 4, Box 4.1) was established following an initial regulatory sandbox by the data processor and the UK DPP authority, which enabled an assessment of key data protection issues. The use of a pilot programme allowed participants to assess the results, and consider areas for improvement in future projects. The safeFBDC and EuroDaT case studies in Germany (Section 4, Box 4.7 and 4.8) reflect the inclusion of the AML/CFT use-case in broader government initiatives to pilot digital solutions to share information while respecting DPP requirements. The Estonian AML Bridge case study (Section 4, Box 4.6) also included government involvement to set and reform the government's data management frameworks. **AML/CFT authorities should engage with other stakeholders (including authorities responsible for innovation, technology or digital policy or academics/experts) to understand the latest developments and encourage broader information sharing pilot programmes to consider including AML/CFT use-cases.**

- **Devise a national AML/CFT/CPF information sharing strategy**, highlighting the priority areas of financial crime or typologies, or the key data types that would benefit most from sharing (e.g., with input from law enforcement authorities and the FIU). This would provide guidance to interested private sector institutions in developing sharing initiatives that align with national AML/CFT/CPF strategy, or results identified in national risk assessments. For example, the use-case of Singapore (COSMIC) demonstrates how information sharing is targeting the three priority risk areas identified by the national risk assessment process and AML/CFT/CPF strategies (Section 4, Box 4.2). Similarly, the use-case of the Netherlands (TMNL) aligns with the National Action Plan against Money Laundering that includes national initiatives on increased exchange of data with

a view to strengthening fraud and ML investigation and prosecution (Section 4, Box 4.3).[41]

- **Identify a leading or co-ordinating agency and establish a contact point on private sector information sharing for stakeholders**. For example, this can be through an existing stakeholder engagement contact point or forum, such as a public-private partnership (PPP). The responsible contact point should consider taking a role in establishing contact and maintaining dialogue with DPP and other government departments, such as digital innovation, to allow consistent advice to be given to private sector stakeholders. Close engagement will also help identify whether an information sharing initiative is creating any risk displacement to non-involved institutions and allow the government to respond to such risks (e.g., by encouraging participation from all regulated entities). Based on the focus group discussions, the degree of involvement by public sector authorities can vary. For example, Singapore's COSMIC case study (Section 4, Box 4.2) illustrates how the AML/CFT/CPF competent authority (the supervisor, MAS) led the development of the sharing initiative. Whereas the UK's case study (Section 4, Box 4.1) illustrates how the UK DPP authority (the ICO) took an active role in engaging with the proponent of the sharing initiative. In Estonia's AML Bridge (Section 4, Box 4.6), a few Estonian authorities (including the DPP authority, the FIU, and the Financial Supervision Authority) participate in the Steering Committee and/or act in an advisory capacity for the initiative.
- **Provide guidance, checklists, or other reference materials setting out the relevant legal/supervisory provisions governing information exchange**. This would assist private sector institutions in navigating the different requirements at a national level. Feedback from the private sector indicates that guidance or interpretative material is also useful to provide clarity on the scope of any exemptions or exceptions, particularly as this related to ML. For example, where sharing is permitted to detect or investigate fraud, to what extent can institutions share information on related ML? Or, conversely, where sharing is permitted to detect or investigate ML, to what extent can institutions share information related to predicate offences? Where guidance is issued, AML/CFT/CPF and DPP authorities should ensure that it is consistent and collaborative, and not issued in isolation. For example, the Estonian AML/CFT/CPF and DPP authorities serve as advisors to the AML Bridge sharing initiative and participate in the project steering group to provide feedback and guidance, along with the product management team and other private sector stakeholders in the steering group (Section 4, Box 4.6). Where the legal framework permits, authorities could also consider going beyond guidance to certify specific data processing arrangements. For example, the Netherland's IAS system operates under a certification from the data protection authority (Section 4, Box 4.4), and the Canadian Consumer Privacy Protection Act similarly gives the Privacy Commissioner the ability to approve a Code of Practice for a data processing arrangement.
- **Explore the feasibility of building a secured platform for private sector information sharing**. This is the most direct approach in providing the necessary

41 www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/plan-van-aanpak-witwassen

financial and technological resources required for information sharing. This approach may also help ensure data sharing initiatives are accessible and affordable for smaller institutions, including those outside the financial sector, which reduces the risk of risk displacement where data sharing initiatives are limited to major institutions. Such a platform could also pave the way for public-private sharing at a national level or a cross-border use in the long run (although these are not currently requirements under the FATF Standards, except in the context of group-wide information sharing). For example, the COSMIC information-sharing initiative of Singapore (Section 4, Box 4.2) and Estonia's AML Bridge (Section 4, Box 4.6) are secure digital platforms that allow (or will allow) sharing and communication among participating financial institutions. In Germany's safeFBDC and EuroDaT cae studies (Section 4, Box 4.7 and 4.8), authorites are involved in the initiatives to develop a platform or trustee to enable information sharing. When building such platforms, governments and participants could consider using standardised or open-source technology for data security and/or making use of technology that meets relevant public certifications to promote trust in data security.

- **Develop projects to promote data interoperability and consistency**. These initiatives may include making available common data standards and definitions, or other data cleaning or structuring initiatives for AML/CFT/CPF data or entries used in STRs. Led by AML/CFT/CPF authorities (e.g. supervisors or the FIU) or digital innovation departments, these initiatives could shorten the time and efforts of data preparation and allow faster implementation of sharing initiatives by interested private sector institutions. Based on experiences learnt from use-cases, some countries (e.g. Singapore) conducted separate exercises to harmonise data formats a few years prior to the implementation of the sharing initiative.

Public sector should ensure and promote regular dialogue between DPP and AML/CFT/CPF authorities

54. In addition, regular, open dialogue between DPP authorities and AML/CFT/CPF authorities (and other financial service regulators) is important to give interested private sector entities greater clarity on how to harmonise policy objectives in practice. In many of the more advanced sharing initiatives covered in the previous section, the leading AML/CFT/CPF authorities have engaged or included their DPP counterparts in regular meetings to discuss solutions or other measures to facilitate private sector sharing initiatives, as well as to identify areas of potential inconsistency or lack of clarity. As set out in the Phase 1 Stocktake Report and FATF's Recommendation 2, national co-operation and co-ordination for AML/CFT/CPF requires interaction between AML and DPP authorities to ensure the compatibility of AML/CFT/CPF requirements with DPP rules and other similar provisions. This dialogue is also vital for an educational purpose, to ensure AML authorities understand the scope, nature and important objectives of the relevant DPP framework and requirements, and vice versa.

55. Collaboration and co-ordination at the international level (both bilateral and multilateral) can help share lessons, encourage discussion and promote consistency in cross-border sharing, in line with the required protection of data. In addition to such operational collaboration, government outreach and consultation efforts could extend to relevant civil society groups (e.g., NPOs or other advocacy organisations with a DPP focus or working on financial exclusion issues), in order to provide

assurance that DPP principles will be upheld while meeting AML/CFT/CPF objectives, as well as to address any concerns that information sharing lead to financial exclusion.

56. Other practical suggestions for how authorities could interact include:

- **Regular forums that bring together AML/CFT/CPF authorities, DPP authorities, and private sector institutions** to discuss policy and operational issues on AML and DPP. The sharing of technical and operational challenges will allow authorities to take an informed approach to resolving issues. Such forums also develop stakeholder relationships and increase knowledge of one another's objectives and regulations.
- To move beyond higher level policy discussions, **DPP and AML authorities could also run joint initiatives, such as joint regulatory sandboxes** that allow participants to explore the interplay between DPP and AML/CFT/CPF legislation, or provide joint guidance on how DPP and AML/CFT/CPF legislation interacts.
- To encourage industry initiatives, **AML/CFT/CPF authorities could co-ordinate with DPP authorities to devise a strategy on information sharing** and to promote private sector information sharing that is protected with proper safeguards (in terms of digital security and data protection/privacy).
- **DPP authorities could provide guidance or other support**, such as for technological solutions to share data while reducing DPP risks (e.g., minimising the personal data shared or pseudonymising the data) or to conduct sector-wide engagement concerning data sharing to allow a holistic understanding of the DPP requirements.
- **AML/CFT/CPF and DPP authorities could consider joint guidance** or statements or other communications to ensure greater policy harmonisation. If countries pursue legislative gateways, AML authorities should work closely with DPP authorities to ensure coherence of laws and requirements.
- **AML authorities should facilitate industry engagement with DPP authorities as appropriate**. It may be useful to include DPP in private sector consulation or sector-wide engagement.

Recommendations relevant to the private sector:

Private sector should consider the application of PETs

57. PETs can help support compliance with DPP requirements, even if they are not a 'silver bullet' in ensuring compliance with these legal obligations.For example, they can help reduce or eliminate the movement of data, minimise the personal data shared, and pseudonymise, anonymise, or encrypt shared data. The Phase 1 Stocktake Report outlined in detail the various types of technology that could be applied and the risks and opportunities they may pose. As set out in the section above, there may be challenges associated with the scope of data that can be accessed and processed, its accuracy and reliability, and whether relevant stakeholders hold the data in standard formats. Ensuring AML/CFT/CPF experts, technology providers and DPP experts are engaged in any discussions on information sharing initiatives will help ensure that the technical design and output of the initiative is in line with the objectives. This includes ensuring that the PET is

fit-for-purpose and relevant data security risks are managed.[42] PETs also need to be accessible to smaller institutions, which form the majority of obliged entities. For example, the UK's FutureFlow platform (Section 4, Box 4.1) uses pseudonymisation technologies to remove/clean the personal data contained in financial transaction data (such as account identifiers, transaction value(s), transaction ID(s), and timestamps) prior to exchange in order to minimise the risk of re-identification. In considering the use of PETs, it is also important to pay attention to the interoperability of different technologies (e.g., by using technologies that confirm to accepted standards) to allow broader engagement. Where used appropriately and in line with DPP rules and obligations, PETs and AI technology have the potential to enable more accurate, reliable, objective and secure processing.

Private sector should take steps towards data preparation

58. New data-sharing or data-pooling technologies, especially advanced analytics, work best with common data standards and formats. Interoperable data formats and structures also help improve data accuracy and reliability, hence addressing some of the data-related challenges identified in the previous section. Private sector institutions could consider a number of strategies, including: making use of existing available data prepared in structured format (e.g. data fields used in SWIFT); introducing data cleansing initiatives prior to sharing; or assigning technology providers to plan and implement data cleansing/structuring initiatives (particularly if they are a participant in the information sharing initiative). In the UK's TriBank Initiative (Section 4, Box 4.1), participating financial institutions had to spend a significant amount of time during the early stages of the project to ensure all participants could share data seamlessly through the digital platform. Estonia's AML Bridge (Section 4, Box 4.6) also noted that significant time and effort was spend resolving less visible challenges, which may include issues like data preparedness.

Private sector should pursue data protection by design

59. Considering DPP principles in the design phase of an information sharing initiative is key to its success. To this end privacy risk assessments/Data Protection Impact Assessments (DPIAs) provide an analytical framework to assist stakeholders in assessing DPP compliance and identifying and mitigating potential DPP risks (see the box below). The examples of advanced initiatives above demonstrate that the legal basis for sharing/processing/storing personal data and the mitigation measures put in place should be tailored to the project, its objectives and the use/processing of data. Where applicable, a proper assessment of relevant suitable legal bases should also be undertaken. In most cases, each individual financial institution will need to develop its own DPIA considering its own data collection and processing policies, although a DPIA could be developed jointly by the participating institutions, noting any differences between institutions.[43] In one of the projects described above, the lead stakeholder (i.e., the digital platform provider) engaged

---

42 See: European Union Agency for Cybersecurity (2021) *Data Pseudonymisation: Advanced Techniques and Use Cases*; European Union Agency for Cybersecurity (2019) *Pseudonymisation techniques and best practices*.

43 In some jurisdictions, public authorities may also be subject to an obligation to submit a DPIA, depending on their role and involvement in the initiative.

with the DPP authority and developed a working model of a DPIA to reduce the resource burden on participating financial institutions.[44] Taking data protection into account at the beginning stage of the project also allows participants to pivot projects to align with relevant DPP requirements, thereby saving resources.

Box 6.1. What should a Data Protection Impact Assessment (DPIA) include?

The exact requirements for a DPIA will depend on the relevant DPP legislation and features of the sharing initiative(s), but could include the following:

- Specific purposes and goals of the project.
- Identification of a legal authority/basis that authorises or compels the parties to engage in these ML/TF/PF detection and investigation arrangements, and in-depth verification of conditions that meet the legal basis.
- An analysis of whether or not other arrangements could achieve similar results or the intended benefits of the project.
- Clarify which parties are undertaking key data protection roles in respect of the data utilised (e.g. who is a controller, joint controller and/or processor), note any contracts between data controllers and processors.
- A description of how the parties will collect, use, disclose/share, store, and later delete or otherwise destroy the data.
- Specific data points/elements that will be shared, pooled, analysed or otherwise processed for the project, including whether data is pseudonymised or anonymised at any stage of the project and, if so, when/if re-identification is possible and by which entity. Particular attention should be given to data of a sensitive nature or in a special category (under the relevant DPP framework).
- Common data standards and interoperability.
- How to ensure data quality, accuracy and adequacy as needed in the context of the initiative, and data minimisation. In line with the data minimisation principle, initiatives may wish to consider adopting a graduated approach from the outset, while ensuring the data shared is sufficient and adequate to meet the purpose of sharing. E.g., institutions could consider lower-risk models or options as pilot cases, and expanding this as necessary and permissible based on effectiveness. Adherence to the adequacy principle, in conjunction with appropriate data minimisation, will help to ensure effective data sharing.
- If and how sharing or pooling and/or analysis or processing of the data elements will occur.
- If data will be collaboratively pooled or shared, how security of the data will be guaranteed from the initial transfer into the pool, throughout its use in the pool, through deletion/destruction of the data when appropriate, and in the

[44] An example of a DPIA used by the FutureFlow platform (Section 4, Box 4.2) is available on the FATF website.

event of loss or unauthorised disclosure of the data, description of risk mitigation measures, including notification to relevant authorities and possibly data subjects that may be impacted.

- Mapping of data flows to ensure clear understanding.
- Implications for cross-border or international transfers of data.
- Privacy risks that arise from the arrangement, and mitigation measures.
- Any implications for vulnerable or marginalised groups.
- Mitigation measures (such as technical, legal and organisational safeguards) to address risks in the application of new technology on individuals, including:
  - Measures that could or will be implemented to minimise risks of false positives.
  - Measures to mitigate potential adverse impacts on individuals (e.g. what measures need to be in place to help ensure that individuals are not unfairly denied access to services and to help ensure a right of appeal).
  - Other measures to mitigate risks to the rights/freedoms of data subjects.
- Questions of transparency and providing data to individuals, including how to prevent tipping off.

60. In addition to DPIAs, entities involved in data sharing agreements could consider undertaking or adopting:

- Data sharing agreements/contracts, setting out the responsibilities of each party, including to provide a clear framework for dealing with customer complaints or the exercise of individual's rights (including under the relevant DPP laws).
- Human Rights Impact Assessments (HRIAs), which provide a useful mechanism to mitigate the risks to individuals and ensure all actors comply with human rights obligations (such as the right to privacy), e.g., for sharing initiatives involving AI surveillance.[45]
- Legitimate Interest Assessments (where data is shared on the basis of 'legitimate interest'; see Section 3). These help data controllers identify a legitimate interest, ascertain whether processing is necessary to achieve this interest, and then balance the interest against the data subjects' interests, rights and freedoms.

Private sector should establish early and ongoing engagement with DPAs

61. Involvement of DPP authorities from the beginning of any information-sharing project is often critical and beneficial to the success of a private-sector AML/CFT/CPF information sharing project. Regular and transparent communication with the applicable DPP authorities can help navigate unexpected challenges and assess any new risks as they emerge. Ideally, this engagement would begin as the financial institutions are designing their approach to collaboration and improved detection of ML/TF/PF, and would continue through the preparation of

[45] See: Danish Institute for Human Rights (2020) Guidance on Human Rights Impact Assessment of Digital Activities

the DPIA and on an ongoing basis as the project moves forward and data collection and analytics begin. Involvement of the AML/CFT/CPF authorities can also be critical in the success of private sector-led initiatives. For example, the UK public authorities, such as the Financial Conduct Authority (FCA), are required to consult the Data Protection Authority during the preparation of legislative measures that involve processing of personal data (UK GDPR, article 36(4)). This ensures early engagement to identify risks and put in place corresponding mitigating measures. The Estonian sharing initiative (AML Bridge: Section 4, Box 4.6) has invited DPP authorities to join the project and provide advice and input as part of the steering group. In the early stages of the project, fortnightly meetings were held in order to obtain immediate feedback, which in turn allowed timely adjustment to the design of the sharing initiative.

Private sector should develop indicators and metrics to measure success

62. Setting clear performance indicators or metrics to assess results and measure success is important for ensuring that information sharing initiatives reach their goals. For example, at the time of finalising this report, COSMIC project participants (Section 4, Box 4.2) are in the process of discussing specific key performance indicators to measure the project's success, such as the number of STRs filed/customers exited/prospects stopped from onboarding due to COSMIC info, timeliness to respond and identify a suspicious network, number of cases detected by COSMIC that lead to LEA action/prosecution, etc. Collecting clear qualitative or quantitative information enables participants to determine whether the initiative is achieving its purpose and continually reassess whether the information sharing is necessary/reasonable/proportionate. Sharing positive results also helps build trust in initiatives, and can help encourage the inclusion of a wider range of participants (where in line with DPP rules).

Private sector should adopt measures to prevent de-risking related to information sharing

63. Data obtained through information sharing initiatives may eventually play a part in an institution's decision to exit a relationship or not provide certain services in order to manage ML/TF/PF risk. If these decisions are not taken on a case-by-case basis or based on additional reliable sources of information, this could result in unintended de-risking. Ideally, proper adherence to DPP requirements, particularly around automated decision-making, data quality and accuracy, and the rights of individuals to have inaccurate data corrected, can help minimise these risks. Individual institutions must maintain responsibility for making these decisions and need to undertake their own investigations in order to do so (e.g., it is up to an individual financial institution to decide whether or not to file a STR). Sharing mechanisms can provide a resource in decision-making, but should not be used to outsource such decisions. Institutions involved in private sector information sharing initiatives need to establish, in advance, the relevant procedures or threshold for triggering exiting measures, taking added caution given the potential harm to a customer that is wrongly identified under a private sector information sharing initiative.

ANNEX A:
Further background on AML/CFT/CPF requirements

64. As highlighted in the main report, private sector information sharing initiatives may involve a number of stakeholders that are not familiar with international and national AML/CFT/CPF requirements. This Annex is prepared to provide background information on how FATF Standards are relevant in terms of information sharing. This information is broader than private sector information sharing for the purposes of identifying suspicious transactions and covers various forms of private sector information sharing as relevant for various AML/CFT/CPF purposes.

Introduction to FATF Standards Applicable to Private Sector (Preventive Measures)

65. To comply with the FATF Standards, countries must impose specific obligations on the private sector[46] to mitigate ML/TF risks – collectively known as preventive measures and encompassing FATF Recommendations 9 through 23. Preventive measures are focused on the prevention, detection and reporting of customers and transactions suspected of money laundering, associated predicate offences and terrorist financing. In general, preventive measures require the private sector to:

- understand the nature and level of ML/TF risks and apply AML/CFT policies, internal controls, and programmes as required to adequately mitigate those risks (R.1);
- know who their customers are and monitor their accounts and activities as appropriate for AML/CFT purposes (R.10). This involves customer due diligence (CDD) measures to identify and verify the identity of their customers (commonly referred to as know-your-customer (KYC) requirements) at the time of establishing a customer relationship. It also requires the private sector to understand the purpose and intended nature of the business relationship with that customer. Importantly, CDD also includes conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that they are not being misused for ML/TF.

[46] This refers to financial institutions, designated non-financial business professions (DNBFPs), and virtual asset service providers (VASPs). See the FATF Glossary for specific scope.

- be able to detect and report suspicious transactions (R.20) and comply with other AML/CFT requirements. Financial institutions hold the relevant transaction data and typically have transaction monitoring systems (with automatic risk indicators) in place to identify suspicious transactions within their institution. As ML/TF activity becomes more complex the ability of these systems to effectively identify large-scale or sophisticated schemes is limited without digitalisation, machine learning and greater information sharing.
- keep records on CDD and other transaction information for at least 5 years (R.11) to enable law enforcement investigations as financial crime is often difficult to detect and investigations can take considerable periods of time to reveal complex networks.
- ensure customers are not informed that a suspicious transaction report (STR) or related information is filed with authorities (R.21). These provisions are not intended to inhibit private sector information sharing efforts but STR confidentiality ensures that potential criminals are not alerted to law enforcement authorities to investigate, prosecute and disrupt ML/TF activities. This recommendation also provides safe harbor to financial institutions and their representatives in their good faith efforts to report suspicious transactions.

66. In order to meet their AML/CFT obligations, the private sector must collect, store and share relevant data and information to identify and report suspected ML/TF activities to competent authorities (noting that AML/CFT and DPP authorities have duties to ensure this data satisfies both AML/CFT and DPP requirements). Such data and information will need to be stored properly and be shared securely with (1) public sectors (i.e. supervisors and law enforcement agencies, domestically and occasionally internationally); and (2) private sectors (i.e. within group/foreign branches, with other Financial Institutions or Designated Non-Financial Businesses or Professions in the country) to allow timely and effective disruption of AML/CFT cases. The FATF recently clarified that information sharing is particularly necessary in context of group-wide programmes against ML/TF in order to detect and report sophisticated professional money laundering networks that separate their activities across different entities and jurisdictions in order to facilitate corruption, drug trafficking, tax evasion.[47]

FATF Standards for Information Sharing in Combatting ML, TF and PF

Private to Private Sector AML/CFT/CPF Data Sharing

67. The FATF has previously issued **guidance** on the type of data and information sharing **within financial groups** necessary to the effective application of the risk-based approach.[48] The table below details the types of information that are shared within financial groups, and explains the broad AML/CFT purposes that such sharing seeks to achieve.

47 The FATF has published guidance on information sharing and the application of FATF Standards for group-wide programmes against ML/TF by financial institutions and DNFBPs.

48 FATF Guidance on Private Sector Information Sharing (November 2017)

Table A1. Types of information shared within financial groups for AML/CFT/CPF purposes

Types of Information	Examples of information elements (as available, when necessary	AML/CFT/CPF purposes for sharing information within the group
Customer Information	Customer identification and contact information (name and identifier), in case of legal persons and arrangements: information on nature of its business and its ownership and control structure; legal form and proof of existence; address of registered office and principal place of business; Legal Entity Identifier (LEI) information, financial assets records, tax records, real estate holdings, information on source of funds and wealth, economic/professional activity, and account files, whether the customer is a PEP (including close associates or family members) or not and other relevant elements from documents collected while on-boarding the customer or updating records, targeted financial sanction information and any adverse information, whether identified from public sources or through internal investigation relating to ML/TF, risk categorisation of customer etc.	Manage customer and geographical risks, identify global risk exposure as a result of on-boarding of the same customer by multiple entities within the group, more efficient record-keeping of customer information.
Beneficial Owner Information	Beneficial owner identification and contact information, real estate holdings, information on source of funds and wealth, economic/professional activity, and account files, whether the beneficial owner is a PEP or not and other relevant elements from documents collected while on-boarding a customer or updating records	Manage beneficial owner and geographical risks, identify the same beneficial owner for multiple entities within the group, more efficient record-keeping of beneficial owner information.
Account Information	Bank/other account details, including the intended purpose of the account, expected location of transactions/activity as expressed by the customer and business correspondence etc.	Effective due diligence and transaction monitoring at group level, justification of transaction pattern vis à vis financial profile, follow-up on any alerts or abnormal trading pattern across the group

Types of Information	Examples of information elements (as available, when necessary	AML/CFT/CPF purposes for sharing information within the group
Transaction Information	Transaction records, credit and debit card records and usage, past credit history, digital footprints (IP address, ATM usage information etc.), attempted/failed transaction information, currency transaction reports, information on closure of account or termination of business relationship due to suspicion, analysis made to detect unusual or suspicious transactions etc	Global transaction monitoring, alert processing and identifying suspicious transactions, flagging and checking the existence of similar behaviour across business lines within the group.

68. The FATF requires that "Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management."[49] The table above illustrates the types of data and information sharing within financial groups, but these types of data can also be used for information sharing between financial institutions and financial groups known as Private-to-Private Sector AML/CFT/CPF Data Sharing. The transnational nature of ML/TF/PF activities typically can be more effectively identified and mitigated through information sharing and co-ordinated reviews by multiple FIs and financial groups.

Public-Private Partnerships

69. Similarly, information sharing between public and private sector stakeholders through Public-Private Partnerships (PPPs) increase effectiveness of AML/CFT/CPF measures by facilitating a more comprehensive view of transactions and customers' behaviour. Such sharing often happens in a secured environment permitting further data-mining, operational analysis and scanning by the private sector to fill potential intelligence gaps. These PPPs enable information sharing across supervisors, FIU, law enforcement, vetted participants from the private sector as well as international partners in some cases. They highlight some of the tangible benefits of bringing together private sector information to pursue serious crimes.

70. In July 2021, the FATF reviewed the information sharing mechanisms covering PPPs in its report on the "Opportunities and Challenges of New Technologies for AML/CFT." There are a number of PPP initiatives in several countries that demonstrate their utility (see below).

[49] FATF Recommendations, Interpretive Note to Recommendation 18.

Box A1. Concrete results from PPPs

Achievements of the **UK's Joint Money Laundering Intelligence Taskforce (JMLIT)** include:

- Development of financial intelligence on over 400 live cases; and
- Intelligence-led outcomes including, over 100 arrests, the restraint of millions of pounds of criminal assets, the identification of thousands of previously unknown bank accounts and new subjects of interest.
- Worked closely with UKFIU and banks in order to provide 24/7 operational support in response to UK terrorist attacks.
- The submission of high quality SARs, in response to which UKFIU undertook fast track handling, further enhancing law enforcement enquiries.

Achievements of **Australia's Fintel Alliance** include:

- Development of and sharing a typology of financial crime risks relating to the Panama Papers;
- Referral to the Australian Federal Police (AFP) of persons of interest in connection with child exploitation;
- Identification of new suspects involved in serious organised crime;
- Provision of intelligence to the AFP on persons of interest in connection to a foiled terrorist attack targeting an international flight from Sydney; and
- Provision of financial intelligence to the AFP in relation to approximately 600 persons identified as "missing persons".

Achievements of **Canada's project-based PPPs** include:

- The development of new typologies and indicators which have been created in cooperation with the private sector.
- New operational alerts developed in a collaborative manner with the private sector and other government departments through PPP initiatives. These alerts have been shared with reporting entities. These operational alerts include up to date indicators and high-risk factors related to specific methods of ML/TF.
- Significant increases in the quantity and quality of STRs relating to priority activities, and a subsequent increase in the number of disclosures to law enforcement.
- Significant number of FINTRAC briefings to domestic and international audiences, including private sector, law enforcement, and other government agencies.

Achievements of the **Hong Kong China's Fraud & Money Laundering Intelligence Taskforce (FMLIT)**

- Development of financial intelligence on over 150 live cases.
- Intelligence-led outcomes including arrest of 394 criminals, the prevention of dissipation of HKD 749 million in criminal proceeds, and the identification of thousands of previously unknown entities to LEA.
- Development and sharing of typologies/red flag indicators on a wide range of topical financial crimes and ML activities.

Achievements of **Singapore's ACIP** include:

- ACIP best practice papers to mitigate risk areas of trade-based ML (TBML) and misuse of company structures for illicit purposes were well-received by the industry.

- Seminars open to all industry members, to discuss the above-mentioned best practice papers as well as solutions for overcoming key challenges and issues in AML/CFT data analytics.
- Publication of industry perspectives paper to promote effective adoption of AML/CFT data analytics tools, and practice note on mitigating the impact of operational disruptions from COVID-19.
- Development of ACIP advisories to warn the industry of emerging typologies and cases of concern.
- Public-private collaboration on priority investigations that have thus far led to successful interceptions of USD 50 million.

Achievements of **Russia's Compliance Counsel** include:

- A reduction in the use of wire-transfers for TF purposes;
- Development of an identification system, that detects clients, who match the foreign terrorist fighter profile by analysing financial and behavioural patterns;
- Development of a periodically updated system of regional designations that supplies banks with information on individuals wanted within the CIS region and IDs seized by ISIL terrorist-fighters in Iraq, Syria, that are subsequently closely monitored;

Achievements of **U.S. FinCEN Exchange** include:

- Between 2015 and 2018, FinCEN convened over a dozen briefings, in five cities, with over 40 FI participants and involving multiple law enforcement agencies;
- Intelligence-led outcomes including identification of bank accounts, subjects, and networks and information to support arrests, indictments, and seizure warrants;
- Development of new typologies that FinCEN shared industry-wide;
- Informed or supported U.S. Treasury actions, such as sanction designations and Geographic Targeting Orders; and
- Facilitated private-private information sharing pursuant to USA PATRIOT Act Section 314(b).

The preliminary achievements of the only supra-national PPP, the **Europol Financial Intelligence Public Private Partnership (EFIPPP)**, include:

- The use of a dedicated secured platform to share threat assessments and strategic reports by members.
- Collaborative development of three typologies (two on investment fraud and one on a 'correspondent nesting structure' for sanctions evasion and ML purposes) based on on-going cross border investigations, comprising specific geographical indicators. Participants reviewed the typologies to request and/or add further details

PARTNERING IN THE FIGHT AGAINST FINANCIAL CRIME DATA PROTECTION, TECHNOLOGY AND PRIVATE SECTOR INFORMATION SHARING

A single financial institution has only a partial view of transactions and sees one small piece of what is often a large, complex puzzle. Criminals exploit this information gap by using multiple financial institutions within or across jurisdictions to layer their illicit financial flows.

By using collaborative analytics, bringing data together, or developing other sharing initiatives in responsible ways, financial institutions seek to build a clearer picture of the puzzle, to better understand, assess, and mitigate money laundering and terrorist financing risks.

This report aims to help jurisdictions responsibly enhance, design and implement information collaboration initiatives among private sector entities, in accordance with data protection and privacy (DPP) rules, so that the risks associated with increased sharing of personal data are appropriately taken into account. This report complements the FATF's report on Stocktake on Data Pooling, Collaborative Analytics and Data Protection (July 2021).

www.fatf-gafi.org | JULY 2022