Future of Financial Intelligence Sharing (FFIS)

Policy Discussion Paper:
A new era of private sector collaboration to fight economic crime

March 2025

RUSI

FFIS
Future of Financial Intelligence Sharing

A new era of private sector collaboration to fight economic crime

Author: Nick J Maxwell

About

This paper is produced by the Future of Financial Intelligence Sharing (FFIS) research programme as part of our mission to conduct independent research into the role of public-private and private-to-private financial information sharing in detecting, preventing and disrupting crime. The FFIS programme is a research partnership within the Royal United Services Institute (RUSI) Centre for Finance and Security.

Founded in 1831, RUSI is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on securing a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Acknowledgements

The FFIS programme would like to thank all those who contributed to this Discussion Paper and our broader research programme.

Sponsors of this research paper are gratefully acknowledged:

- Deloitte
- FNA
- HSBC
- Mastercard
- Nasdaq Verafin
- Swift

For more details about the FFIS programme, please visit www.future-fis.com.

Citation and use

This paper is made publicly available and is intended to support a public-interest policy debate related to the effectiveness, efficiency and data proportionality of methods and approaches to detect and disrupt economic crime.

All information in this paper was believed to be correct by the author as of 6 January 2025. Nevertheless, the FFIS programme cannot accept responsibility for the consequences of the use of any information contained herein for alternative purposes and other contexts. The views and recommendations expressed in this publication are those of the author and do not reflect the views of RUSI or any other institution.

Reference citation: *Maxwell, N (2025). 'A new era of private sector collaboration to fight economic crime', Future of Financial Intelligence Sharing (FFIS) research programme.*

Contents

Glossary

Mexico Banking Association	ABM
Artificial intelligence	AI
Anti-money laundering, countering the financing of terrorism	AML/CFT
The EU AML Authority Regulation	AMLAR
The EU AML Regulation	AMLR
Authorised push payment fraud	APP
The Bank for International Settlements	BIS
Bank Negara Malaysia	BNM
Singapore's 'Collaborative Sharing of ML/TF Information & Cases'	COSMIC
Counter proliferation financing	CPF
The UK Economic Crime and Corporate Transparency Act	ECCTA
Economic crime-related	ECR
Europol Financial Intelligence Public Private Partnership	EFIPPP
The EU AML Authority	EU AMLA
Fraud attack and scam transaction money laundering	FAST
Financial Action Taskforce	FATF
The Future of Financial Intelligence Sharing	FFIS
Financial Information Sharing Partnership	FISP
Government Financial Intelligence Unit	FIU
Financial Network Analytics Ltd	FNA
Financial Stability Board	FSB
General Data Protection Regulation	GDPR
The J5 Joint Chiefs of Tax Enforcement and the Global Financial Institutions Partnership	GFIP
Swift Industry Pilot Group	IPG
Law Enforcement Agency	LEA
Mexico's Ley de Instituciones de Crédito	LIC
Monetary Authority of Singapore	MAS
Malaysia's 'National Fraud Portal'	NFP
National Risk Assessment	NRA
Private-to-private	P2P
Payments Network Malaysia	PayNet
Canada's Proceeds of Crime and Terrorist Financing Act legislation	PCMLTFA
Privacy enhancing technologies	PETs
Mexico's Plataforma de Intercambio de Información Preventiva	PIIP
Public-public cooperation	PPC
Public-private partnership	PPP
The Royal United Services Institute	RUSI
Mexico's Ministry of Finance	SHCP
The U.S. AML Act	U.S. AMLA

Executive Summary

Welcome to the new era of private sector collaboration to detect economic crime.

Between 2023 and 2024, the UK, Singapore, the EU, Canada and Australia passed legislation to enable private-to-private (P2P) collaboration to detect economic crime risk. The UAE and Hong Kong have raised the prospect of similar legislation, and Mexico and the U.S. have enhanced their pre-existing legislative frameworks with new policy or operational developments in the field of collaboration to fight economic crime.

In Chapter 1 of this study, we compare the respective legislative provisions in the U.S., Mexico, Singapore, the UK, the EU and Canada with respect to: whether the information sharing is compulsory or voluntary; what type of data can be shared; the economic crime threat domain coverage; the type of private sector entity that can participate; the legal threshold for sharing and purpose limitations; public sector involvement in the sharing; the threat prioritisation process; and whether the legislation includes an enabling provision for cross-border information sharing. We are concerned in this study with P2P information sharing between obliged entities, rather than within a financial group.

We also compare whether other legal provisions in the respective jurisdictions, beyond the AML P2P legislation in question, allow for operational public-private information sharing on economic crime threats and – crucially – whether AML P2P information sharing is supported by the process of anti-money laundering supervision.

Comparing six legislative environments for AML private-to-private information sharing

We find that the range of entities that can engage in the information sharing varies from just six banks (in Singapore); to all banks (in Mexico)[1]; to all financial institutions (in the U.S. 314(b) associations); to a subset of AML obliged entities (under the UK 'indirect sharing' legal provision); to all AML obliged entities (in the EU and Canada).

Across the six jurisdictions surveyed, the threshold for sharing differs from requiring 'safeguarding action to be taken' by an obliged entity prior to sharing (UK 'indirect sharing'); to requiring compliance with a set of conditions that includes whether sharing the information could help determine whether a customer is 'higher risk' (in the EU); from relying on indicators that are published by the government (Singapore); to whether the sharing is reasonable and subject to a code of practice (in Canada); to where there is no specific threshold or trigger set of conditions stated in law before information sharing can take place (such as in the U.S. and Mexico).

The collaboration frameworks vary in terms of how threats are prioritised; from specific, government-directed use-cases (Singapore); to an emphasis on national or EU risk assessment priorities (EU); to a potential link, through the U.S. AML Act, to national priorities (in the U.S.); to no particular threat priorities directed within the law (as in Canada, the UK and Mexico).

We then compare how the legislation varies in terms of what specific information sharing capabilities they permit.

We survey the following capabilities and make assessments as to what is permissible under the legal frameworks:

- Data-driven collaborative development of typologies of economic crime threats;
- Messaging communication (bi-lateral);
- Messaging communication (multiparty and via a platform);
- Intelligence development at the level of a multi-party platform, to identify risk that no individual participant had otherwise observed;
- Joint case investigations by members (private sector only);
- Collaborative intelligence and joint investigations by members (with law enforcement or investigative agency input);
- A warning function, one to many (i.e. an adverse incident database);
- A tracing function to identify exposure to money laundering/muling dispersals (i.e. a rapid or automated warning chain of alerts to follow transactions across multiple obliged entities, illuminating the network of accounts involved in a dispersal); and
- Combined transaction monitoring for partnership members.

The role of supervisors and policy-makers

A key challenge in 2025 relates to the incentives for collaboration. Most of the legal gateways created are voluntary and, at present, largely inconsequential for AML supervisors. Even as collaboration demonstrates more effective results, the incentive structure created by supervisors for a private entity to invest in such collaboration remains weak.

We argue that significant changes are now required by supervisors to adapt to the new era of collaboration. We urge supervisors to consider their role in encouraging effective outcomes from the private sector and, accordingly, their role in stimulating private sector activity and investment in private sector collaboration and data-sharing.

We highlight that the growth of private sector information sharing raises the prospect of greater consistency between obliged entities in terms of customers being denied services. We emphasise that this brings a policy conflict into sharper focus as to: (1) whether there is a right to financial services; and (2) whether it is appropriate to exclude individuals from financial services based on suspicion of financial crimes.

Ultimately, this policy conflict is unresolved at the international standards level and by domestic policy-makers. Private-to-private information sharing platforms are not in a position to resolve it for policy-makers. Policy-makers will need to determine whether financial exclusion is an appropriate response to suspicion of financial crime and, if so, what the threshold for exclusion should be.

We argue that policy-makers should also take an active role in ensuring that adequate processes are in place to hold private-to-private AML information sharing accountable. It is a responsibility of both public sector and private sector decision-makers involved in AML information sharing to avoid harm to innocent parties and establish a clear complaints and redress pathway to allow citizens to both challenge the accuracy of a determination of risk (assigned to them) and seek data correction, where appropriate.

At this point, AML/CFT policy-makers have been relatively unclear about how 'sticky' a determination of risk should be and, indeed, what the pathway is for a citizen to be rehabilitated into the financial system from an AML perspective.

Collaboration platforms are tools that can support more effective and comprehensive intelligence development and can also facilitate more consistent 'preventative measures' across participant obliged entities. Such platforms can assist obliged entities to achieve the intent of policy-makers in a more effective, efficient and comprehensive way. However, this presents a need to ensure that policy-makers are clear about what their intent is and how tensions are balanced and resolved with regard to financial exclusion vis-a-vis financial inclusion and relevant consumer rights issues.

The next frontier

In Chapter 2, we bring the discussion to the cross-border level.

While the policy consensus to enable private sector entities to collaborate in response to economic crime threats is now well established at the domestic level in major economies and financial centres, policy discussions about cross-border private sector collaborations are less well developed – particularly in the fraud and scams domain of economic crime risk.

The maturity of the policy framework for cross-border information sharing varies considerably between the different domains of economic crime, with cyber-crime arguably the most developed.

We make a case that fraud and scams – as predicate crimes leading to money laundering – are the strongest candidates to focus on in terms of developing a cross-border information sharing framework.

This is because:

(1) the level of certainty that the information relates to a crime having taken place is often very strong in cases where there is a reported fraud (an authorised push payment fraud or scam (APP)) and there is an identified victim (in contrast to other money laundering predicate crimes, which are typically based on identifying suspicion); and

(2) to date, there has been a distinct lack of an inter-governmental forum or standards-setting process for how fraud and scams risk information is collected and shared to respond to cross-border threats (in contrast to the highly developed AML/CFT standards-setting framework developed through the FATF).

We set out 10 innovation track options for enhancing the cross-border legal, policy and operational environment for economic crime risk collaboration.

We argue that policy-makers, supervisors and industry leaders should now take inspiration from initiatives at the domestic level related to private sector collaboration and explore how the same benefits could be achieved at a cross-border level, with robust governance protocols and privacy standards.

The new era of private sector collaboration is just beginning.

In this new era, there is a promise of achieving a more effective, a more efficient and – even – a more data proportionate response to how economic crime is tackled. With greater understanding about the legislation and the development of a wider enabling environment for collaboration, participants have an opportunity to realise this promise.

It is the author's intent that this paper can help to support policy-makers, supervisors and industry leaders in that journey to implement information sharing effectively, safely and in an accountable manner at the domestic level and to advance cross-border innovation in terms of 'connecting the dots' of risk awareness that is being developed at the national level.

Introduction

This paper builds from the FFIS *'Lessons in private-private financial information sharing to detect and disrupt crime'* Survey and Policy Discussion Paper (July 2022)[2], which surveyed 15 different platforms for private-private collaboration. The survey identified the impact of collaboration initiatives – operating across the economic crime domains of anti-money laundering, countering the financing of terrorism (AML/CFT) and/or fraud – where multiple financial institutions (or 'obliged entities' under a national AML regime) come together to share financial data.

The 2022 FFIS paper analysed several barriers to establishing such collaborative analytical platforms and, in particular, highlighted the need for clear legislative frameworks to enable private-private financial information sharing.

Since that time, a number of countries have put forward or enacted legislative reforms which support such information sharing – particularly with respect to AML related private-to-private sector sharing and collaboration.

This paper analyses these developments to:

a) **Provide** a reference resource to understand the international policy and legal landscape with regard to collaboration to detect economic crime in 2025;

b) **Compare** legal approaches in the U.S., Mexico, Singapore, the UK, the EU and Canada;

c) **Describe** key enabling factors for partnership growth and the role for the public sector; and

d) **Highlight** innovation track options to elevate private-to-private economic crime risk information sharing to the cross-border level.

Definitions

In this study we refer to different forms of organisation, as follows:

- **Collaboration:** a broader definition of any attempt to share insight related to any economic crime threats, however brief or transitory.
- **Partnership or a 'Financial Information Sharing Partnership (FISP)':** a specific institutionalised form of collaboration, with a governance framework and some level of permanence to its existence. A 'Partnership' or a FISP could refer to private-to-private (P2P) or a public-private partnership (PPP). In general, we do not focus on public-public cooperation (PPC) between government agencies in this paper. Increasingly, the divide between P2P and PPP is reducing as public agencies seek to draw greater law enforcement or crime prevention benefits from P2P partnerships.
- **Platforms**: refers to the process, technology solution or data intermediary that allows for information relevant to the detection or investigation of economic crime to be shared between two or more members (typically financial institutions) of the platform. Multiple partnerships could be served by the same platform.

In general, the scope of threat activity that we consider in this paper is **'economic crime'** and we use the same definition as laid out in the 'UK Economic Crime Plan 2019-2022'[3], i.e. that economic crime refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others. The definition is broader than 'financial crime' or 'white-collar crime' and covers the following types of criminality:

- the laundering of proceeds of all crimes;
- fraud and scams, affecting the private sector and public sector;
- terrorist financing;
- sanctions evasion;
- market abuse;
- corruption and bribery;
- tax crimes;
- counter proliferation financing; and
- the recovery of criminal and terrorist assets is also in scope.

We use the descriptor 'economic crime-related (ECR)' when we are referring to collaboration or partnerships that may cover one or more of the underlying economic crime threats, and we refer to a specific economic crime threat when we are making a point that is only relevant to a specific threat.

This study focuses on two main domains of economic crime: money laundering (in general) and the specific qualities of money-laundering related to the proceeds of fraud and scams. We also make reference to countering the financing of terrorism (CFT), counter proliferation financing (CPF), sanctions evasion, tax evasion and cyber security threats. We draw from experience across those domains in terms of private-to-private, public-private and public-public information sharing advances.

Fraud and scams have a close relationship with money laundering. The act of money laundering through a financial account can be considered fraudulent use of that account and the proceeds of fraud and scams will, almost immediately, be moved and laundered through financial and payment systems. However, historically, fraud and scams have been treated differently in legislative environments and regulatory obligations compared to money laundering. Fraud and scams are typically cyber-enabled and, therefore, they also have a close link to conceptions of 'cyber-crime'. Whereas some money laundering activity relates to the profit from an illicit trade and the sale of illicit goods to 'consumers' (such as narcotics or counterfeit goods), fraud and scams typically involve a clearly identifiable victim who has been the subject of a theft. In this paper we refer to fraud attack and scam transaction money laundering (FAST money laundering) as deserving of particular attention given the unique opportunities for P2P information sharing related to FAST money laundering.

Our general interest in this paper is on collaboration related to the detection and sharing of **threat and risk** information, rather than utilities for the transparency of general customer data or general payment information or, indeed, for shared know-your-customer (KYC) facilities or identity-verification processes. However, threat-focused information sharing would likely have a complementary role in such identity verification processes. We use the EU terminology of 'obliged entities' for any private sector entity which is obliged to meet AML regulatory requirements. Please note that the breadth of business sectors that are obliged under AML rules can vary from country to country.

Chapter 1.

Recent legislative changes to support private sector collaboration to detect economic crime risk

1.1. The context for policy change to enable private-to-private collaboration

Innovation and legislation to support ECR collaboration has developed significantly, particularly in the AML domain, in recent years.

The FFIS paper '*Five Years of Growth of Public-Private Partnerships to Fight Economic Crime'* (2020) surveyed the rise of 23 different domestic and cross-border PPPs that developed around the world after 2015.[4] Since 2020, we have observed an accompanying level of interest in innovation and policy reform to support P2P collaboration, charted in the FFIS Survey and Policy Discussion Paper: '*Lessons in private-private financial information sharing to detect and disrupt crime'* (2022).[5]

In 2017, the FATF published a range of resources that related to information sharing, including the *'Consolidated FATF Standards on Information Sharing'*[6] (last updated in 2017) and the *'FATF Guidance on Private Sector Information Sharing'*.[7] However, the extent of information sharing covered in those papers – considering sharing between different financial institutions, which are not part of the same financial group – related to Recommendation 13 (correspondent banking), Recommendation 14 (money value transfer services), Recommendation 16 (wire transfer/payment transparency) and Recommendation 17 (third party reliance) of the FATF standards. These recommendations did not, by themselves, require or enable obliged entities to cooperate with one another to communicate risk information or detect AML/CFT risk, though there was encouragement for countries to innovate and explore the benefits of this type of collaboration.[8]

A key driver for legislative changes to enable such collaboration came in 2022, with the publication of the FATF best-practices report, under the German presidency of FATF, entitled *'Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing'* (July 2022).[9] The paper recommended that relevant public sector AML/CFT decision-makers should:

1. Take an active role in facilitating private-private information sharing initiatives;
2. Examine the need for specific legal gateways for such information sharing;
3. Develop an AML information sharing strategy;
4. Support innovation and sandbox initiatives; and
5. Explore the feasibility of public sector support for a specific secure platform for private sector information sharing to take place within.

In the same FATF best-practices paper, private sector stakeholders were encouraged to develop collaboration innovation, including through the application of privacy enhancing technologies and strengthening data interoperability. Obliged entities were called on to pursue 'data-protection by design' and prevent excessive or unwarranted de-risking through collaboration.

Driven by this activity, between 2022 and 2024, a number of countries have updated, enacted or committed to legislation to enable collaboration between obliged entities to detect and prevent relevant economic crime threats. This FFIS paper examines that legislative growth.

In terms of recent legislative changes, in this paper we focus on:

Table 1. P2P legal frameworks covered in this paper

	The U.S. AML Act (2021) and its impact on the original P2P legislative framework in the U.S. established through Section 314(b) of the USA PATRIOT Act (2001).
	Article 115 Bis[1] of the Ley de Instituciones de Crédito (LIC) in Mexico (2008, with updates to the accompanying AML/CFT rules (Chapter XIII) in 2022 and 2024)
	The Singapore Financial Services and Markets (Amendment) Act (2023), enabling the 'Collaborative Sharing of ML/TF Information & Cases' COSMIC platform in Singapore.
	The UK Economic Crime and Corporate Transparency Act (2023), enabling 'direct' and 'indirect' sharing for ECR purposes.
	The EU Anti-Money Laundering Regulation, Article 75 (2024), enabling information sharing partnerships for obliged entities under the EU's AML regime.
	Canadian (Federal Law) Section 11.01 Amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (2024).

Box 1: Australian AML/CTF reforms in 2024

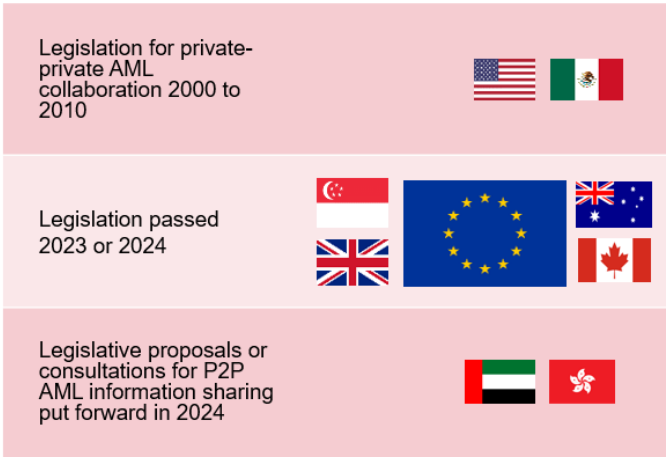
On 29 November 2024, the Parliament of Australia passed the AML/CTF Amendment Bill 2024,[10] amending the Australian AML/CTF Act to amend the prohibition on 'tipping off' customers regarding the reporting of suspicions of unlawful activity. According to the AUSTRAC overview of the changes to tipping-off, *"The reform is intended to facilitate information sharing within reporting groups while ensuring the integrity of investigations…. These changes focus on the harm to be prevented, specifically disclosures that would reasonably prejudice an investigation, while allowing legitimate information sharing within reporting groups and where information is appropriately protected."*[11] The changes create an exception to the 'tipping-off' prohibition for disclosures made to another reporting entity and when the disclosure is made for the purpose of detecting, deterring or disrupting money laundering, the financing of terrorism, proliferation financing, or other serious crimes.[12] These changes will come into effect on 31 March 2025.

While the six jurisdictions covered in detail in this report have set out a positive enabling framework for P2P AML information sharing, including specific enabling provisions and accompanying conditions related to the information sharing, the Australian approach is to remove the criminal penalty that may have otherwise arisen if P2P information sharing was considered to be 'tipping-off'. It is expected that the Australian government will produce further guidance on the P2P information sharing regime in Australia. The full implications of the Australian legal change in terms of the precise capabilities that are enabled and how the Australian P2P legal framework relates to the variables analysed in this study will be explored in a further FFIS paper.

[1] ***Note***: Bis is a legislative drafting technique that refers to the second new article placed under the numbered article; enabling a distinct article to be inserted but avoiding all subsequent articles needing to be renumbered.

Other jurisdictions have announced an intent to legislate to enable ECR collaboration, including Hong Kong SAR and the UAE, or have supported innovation initiatives to explore collaboration opportunities and/or the use of privacy enhancing technologies (PETs) in ECR information sharing, such as in Switzerland.[13]

Figure 1. Timeframe of recent developments in P2P ECR information sharing



The USA and Mexico enact legislation to support P2P ECR collaboration.

Singapore, the UK, the EU, Canada and Australia all enact legislation for P2P ECR collaboration.*

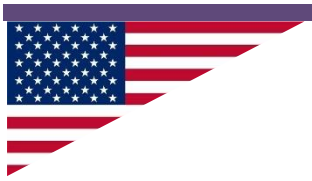
In 2024, Hong Kong and the UAE announced an intent to consider legislation for P2P ECR collaboration.

**In addition, prior to the EU's AML Regulation, EU member states such as Estonia, Latvia and Sweden developed legislative and operational frameworks to encourage P2P ECR information sharing at the domestic level.*

1.2. Understanding the legal frameworks for AML collaboration in the U.S., Mexico, Singapore, UK, the EU and Canada in 2024

In the section below, we describe the new legislative environments for AML collaboration in the U.S., Mexico (currently, the FATF Presidency country, 2024-26); Singapore (FATF Presidency country from 2022-24); the UK and the EU (including Germany, which held the FATF Presidency from 2020-22).

i. USA



USA

Legislative reference and enactment date:	Section 314(b) of the USA PATRIOT Act (2001), relevant implications of U.S. AML Act (2021) and proposed changes to the AML Program Rule (2024). Section 314(b) provides a 'safe harbour' from civil litigation related to P2P information sharing.
Compulsory or voluntary:	Information sharing through 314(b) is voluntary and responses are also voluntary.
Type of data that can be shared:	"Information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals."[14] In reference to the information relevant to a filed Suspicious Activity Report (SAR), "[d]isclosure of underlying facts, transactions, and documents for compliance purposes to an entity outside of an institution's corporate organizational structure may be warranted and would not be prohibited, provided that a SAR or information that would reveal the existence of a SAR was not disclosed."[15]
Economic crime domain coverage:	FinCEN's Fact Sheet of December 2020 clarified that 314(b) is intended by FinCEN to support information sharing on a wide range of ECR unlawful activity – including fraud and cyber-crimes – referred to as 'specified unlawful activity' (SUA).[16]
Type of entity that can participate:	The following types of entities can participate in 314(b) sharing: "Banks, Casinos and Card Clubs, Money Services Businesses, Brokers or Dealers in Securities, Mutual Funds, Insurance Companies, Futures Commission Merchants and Introducing Brokers in Commodities, Dealers in Precious Metals, Precious Stones, or Jewels, Operators of Credit Card Systems, Loan or Finance Companies, [and] Housing Government Sponsored Enterprises."[17]

	314(b) associations – that are not obliged entities themselves – can engage in 314(b) information sharing and perform additional analysis on their members' behalf, enabling multi-party information sharing and more complex collaboration and analysis beyond messaging.[18] However, the types of entities that can be members of 314(b) associations are limited to 'financial institutions'.[19]
Threshold for sharing and purpose limitations:	FinCEN highlight that 314(b) is intended for use by obliged entities for: • Gathering additional information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals. • Shedding more light upon financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions. • Building a more comprehensive and accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring. • Alerting other participating financial institutions to customers of whose suspicious activities they may not have been previously aware. • Facilitating the filing of more comprehensive SARs than would otherwise be filed in the absence of 314(b) information sharing. • Identifying and aiding in the detection of money laundering and terrorist financing methods and schemes. 314(b) does not set an explicit threshold or trigger for information sharing to be lawful. In 314(b) workshops convened by FFIS, 314(b) is generally understood to require an ECR 'alert' as a pre-requisite for sharing and, as such, collaborative transaction monitoring (i.e. direct sharing of large volumes of unalerted customer data) is not part of current 314(b) use.
Public sector involvement:	Information sharing by public authorities, such as law enforcement authorities, is not legislated for within 314(b). Apart from 'housing government sponsored enterprises', 314(b) registration is not open to public agencies to participate in. Instead, public agencies use 314(a) of the PATRIOT Act to facilitate information exchange from competent authorities, or other legislative gateways may be used by law enforcement to share information with the private sector.
Threat prioritisation process:	There is no inherent threat prioritisation set within U.S. 314(b). However, through the U.S. Anti-Money Laundering Act (AMLA), the US Treasury is obliged to publish national AML/CFT priorities on the understanding that financial institutions will be assessed on the extent to which they have reviewed and incorporated these priorities (Sec. 6101).
Cross-border element:	There are no specific enabling features within U.S. 314(b) to share information across borders, however, it is also not prohibited.[20] No FinCEN or federal banking agency regulation prohibits cross-border information sharing – except SARs, or information that would reveal the existence of a SAR – however, the safe harbour for information sharing under 314(b) does not cover information sharing with foreign financial institutions.

There are a number of distinctive features of the USA 314(b) P2P ECR collaboration regime, including:

- **314(b) associations and a network level-view of risk**: 314(b) is a legal authority which protects against civil liability from the relevant sharing. Historically, this has enabled bi-lateral information sharing between 314(b) registered entities. In terms of the shift to multi-party collaborations, FinCEN can authorise the establishment of 314(b) associations. A technology platform can form a 314(b) association and that platform can identify risk by leveraging a network-level 'consortium' view of data; i.e. risk that an individual financial institution within the association would not be able to identify by themselves.

- **Innovative 314(a) and 314(b) connected use:** As previously reported in the FFIS Survey (2022), major financial institutions and law enforcement agencies have worked together to combine 314(a) and 314(b) processes to build collaborative investigative PPPs that can support law enforcement investigations. Numerous positive letters of impact from law enforcement agencies have praised the role of this 'consortium' approach and performance data suggests that law enforcement receives five times more subjects of interest in money laundering investigations by sharing an original set of suspects through this approach.

- **Direct AML supervisor support for AML collaboration:** The U.S. AMLA enables sharing of compliance resources as described in the 2018 statement entitled 'Interagency Statement on Sharing Bank Secrecy Act Resources' (Sec. 6213) and the principal U.S. AML Supervisor, FinCEN, "strongly encourages financial institutions to participate [in 314(b)]."[21] FinCEN has articulated how a culture of compliance may involve, inter alia, effective information sharing.[22] In the 2024 proposed AML Program Rule, FinCEN expects that financial institutions will utilise information obtained from other financial institutions, such as emerging risks and typologies identified through section 314(b) information sharing, to inform their risk assessments. The proposed rule also encourages public-private partnerships and increased communication between financial institutions to ensure that the information financial institutions provide is highly useful to law enforcement and national security efforts.[23]

- **Direct AML supervisor encouragement to cross-border P2P information sharing:** In 2024, FinCEN Director Andrea Gacki stated that "FinCEN encourages U.S. financial institutions to continue to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity."[24] In a July 2024 joint notice with the FBI and OFAC, with regard to Mexico time-share fraud in particular, FinCEN encouraged "U.S. financial institutions to continue to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity. FinCEN also reminds U.S. financial institutions that the sharing of underlying account or transaction information does not violate Suspicious Activity Report (SAR) confidentiality restrictions in the BSA and FinCEN's regulations unless such sharing would potentially reveal the existence of a SAR."[25]

- **High impact in reducing false positives**: 314(b) has significantly reduced false-positive filing. Analysis of more than 82,700 case investigations that took place within the Nasdaq Verafin platform between 2018-2023 (inclusive) – where financial institutions and other entities utilised 314(b) collaboration tools in Nasdaq Verafin's platform – found that 62% of those cases were resolved as 'not suspicious' after an act of communication or collaborative investigation. This indicates that when Nasdaq Verafin members had an initial cause for concern relating to money laundering or suspicious activity and had initiated a communication or collaboration on the matter, they were able to resolve their concern when additional information was available from counterparties in 62% of cases. In these cases, a member has closed their investigation without reaching the threshold of 'suspicion' and therefore a filing would likely not have been required to the government Financial Intelligence Unit (FIU).

ii. Mexico

Mexico

Legislative reference and enactment date:	Under Article 115 Bis within the Mexican Federal Banking Law, Mexico's Ley de Instituciones de Crédito (LIC), and the accompanying 'AML/CFT Rules' (Chapter XIII), set by the Mexican Ministry of Finance (Secretaria de Hacienda y Credito Publico (SHCP)),[26] various AML/CFT information exchange mechanisms are available to Mexican banks, as well as between Mexican banks and foreign financial entities. In this study, we use the term 'Article 115 Bis' to refer, collectively, to the operation of the AML/CFT Rules (Chapter XIII) and the federal LIC legislation in terms of information sharing between obliged entities. Article 115 Bis allows banks to exchange information in order to strengthen measures to prevent and identify acts, omissions or operations that could be related to money laundering or financing of terrorism, without breaching bank secrecy obligations. In 2021, Mexican banks and the ABM established the Plataforma de Intercambio de Información Preventiva (PIIP) as the mechanism to receive and provide information of any crime committed by former employees against the banks or their clients. The banks can only exchange information through authorised officers and are subject to controls to ensure the confidentiality, accuracy and relevance of the information. In 2022 and 2024, Mexican authorities updated the AML/CFT Rules (within Chapter XIII) to clarify that the exchange of information could be carried out through a third-party technology platform and on a multi-party basis.
Compulsory or voluntary:	Information sharing is voluntary, but some elements of responses to requests are mandatory and must take place within 30 days, unless otherwise agreed by the participants.
Type of data that can be shared:	In 2020 and updated in 2024, Mexican banks established specific forms/layouts for information sharing, which included fields for the following types of data: 1. Information related to the entities who participate in the exchange; 2. General information about the client or user whose information is requested; and 3. Specific information on the operation or activity carried out by the client or user (such as: the type and amount of the operation(s), whether the operation is consistent with the knowledge of the client, the client's explanation of the operation, additional information that is known about the operation, user, or recipient, account status, for example).
Economic crime coverage:	Information sharing covers anti-money laundering and terrorist financing.

Type of entity that can participate:	Mexican banks only within LIC Article 115 Bis.[27]
Threshold for sharing and purpose limitations:	There must be an alert related to the customer behaviour before it can be shared through the Article 115 Bis gateway. There are specific conditions set out for each type of sharing under the AML/CFT rules: including when the sharing is between Mexican banks, when sharing within a financial group, when sharing with other foreign financial entities, when relating to internal operations of concern and when sharing blacklist information produced by the Ministry of Finance.
Public sector involvement:	Public sector agencies are not typically involved in the information exchange through Article 115 Bis. However, in Mexico, the Ministry of Finance can issue a blacklist (Lista de Personas Bloqueadas) in order to prevent and detect activities that may be related to money laundering or the financing of terrorism. Banks must cease any activity, transactions or operations with anyone on the blacklist, freeze relevant assets and file a suspicious activity report. In terms of the P2P implications of this blacklist, Mexican banks can share the blacklist with their representative offices, controlling and subsidiary companies, entities of the same financial group and correspondent banks. In the case of information sent to other countries, notice of the exchanged information must be given to Mexican public authorities.
Threat prioritisation:	There is no specific threat prioritisation set out for P2P information sharing in Mexico.
Cross-border element:	Yes. In Mexico, specific provisions support information exchange between Mexican financial institutions and with foreign financial entities. See more details below.

Distinctive features in the Mexican P2P ECR collaboration regime include:

- **The governance P2P domestic information sharing:** The Article 115 Bis AML/CFT Rules (Chapter XIII) set out a clear governance framework requiring that the information exchange is carried out according to the following terms and conditions:

  I. It may be carried out between two or more Mexican banks.

  II. When sending a request, the request can only be issued by individuals who are authorised for such purposes, specifying the reason and the type of information required.

  III. The response to the request for information must be made only by authorised employees and must be made within 30 calendar days from the date on which it was requested, unless otherwise agreed by the participants.

  IV. The information provided in response can be shared with other banks, but only if this is specifically established when making the request.

  V. Banks can proactively share information to other banks, without needing to receive a request.

  VI. Once implemented and operational, the exchange of information shall be carried out through the technological platform established by the banks for this purpose, as well as in accordance with the terms and conditions agreed upon by them, as long as the confidentiality of the information is ensured.

There are specific conditions set out for each type of sharing under the AML/CFT rules: including when the sharing is between Mexican banks, when sharing within a financial group, when sharing with other foreign financial entities, when relating to internal operations of concern and when sharing blacklist information produced by the Ministry of Finance. These conditions are set out in the 62nd AML/CFT Rule 'Bis' to 'Octies' provisions. Banks must keep all the supporting documentation of the exchange, to be made available to the Ministry of Finance (SHCP) and the National Banking and Securities Commission (CNBV).

- **Cross-border element:** In Mexico, specific provisions support information exchange with foreign financial entities (Entidad Financiera Extranjera (EFEs)) since 2015. Pursuant to the 62nd Bis and Ter[2] of the AML/CFT Rules, Mexican banks may exchange information of their customers' and users' operations with similar foreign financial entities, solely and exclusively for the purpose of strengthening the AML/CFT measures. For this purpose, the AML/CFT Rules provide a special mechanism for the exchange, with the following conditions:

  a) The exchange of information must derive from an operation carried out between the Mexican bank and the EFE.

  b) The Mexican bank must enter into a confidentiality agreement with the EFE regarding the shared information, that must contain the position of the employees authorized to receive and send the requests. The CNBV must be notified of the execution of this agreement.

  c) The exchange must be done through the official layout (form) issued by the SHCP, through the Financial Intelligence Unit, for this purpose. The aforementioned official layout was strengthened in 2024.

  d) Prior to or simultaneously with the exchange of information, the Mexican bank must submit to the SHCP – through the official electronic channel (SITI) of the CNBV – a copy of the layout with the exchanged information.

  Pursuant to the 62nd Octies of the AML/CFT Rules, a new official layout was issued by the SHCP in 2024, by means of which Mexican banks can share certain suspicious activity report information with their group, subsidiaries and correspondent banks, as follows:

  i. A confidentiality agreement must be in place, with requirements similar to the one used for the traditional information sharing mechanism and the CNBV must be notified of the agreements.

  ii. The exchange must be carried out through the applicable official layout.

  iii. Information can be shared without request from the counterparty abroad.

- **Recent developments to explore platform use:** In late 2024, a pilot exercise within the banking sector was successfully completed through the 'Veradat' platform to establish confidence in a multi-party platform that enables banks to exchange background information relevant to clients that are flagged by one or more banks as potentially linked to financial crimes. Veradat's platform offers two core functionalities: enabling banks to query customer information across participant institutions to identify matches and access relevant financial crime-related background details, and allowing banks to monitor their client lists to receive real-time alerts when a customer is flagged by another institution. Veradat operates on a decentralized network, ensuring that each bank stores and processes its own data within its security perimeter, while non-matching queries remain undisclosed, preserving confidentiality.

[2] ***Note***: Bis and Ter are legislative drafting techniques that refer to the second and third new articles placed (respectively) under a numbered article; enabling a distinct article to be inserted, but avoiding all subsequent articles needing to be renumbered.

iii. Singapore

Singapore

Legislative reference and enactment date:	On 9 May 2023, the Financial Services and Markets (Amendment) Bill was passed in the Singapore Parliament, providing the legal framework for financial institutions to share information on customers whose profile or behaviour exhibits potential financial crime concerns through a secure digital platform called COSMIC (short for "Collaborative Sharing of ML/TF Information & Cases").[28] These measures came into force in April 2024.
Compulsory or voluntary:	Initiating a request through COSMIC is voluntary, though responses to requests are mandatory. It is envisaged that, in later stages of development, aspects of both the contribution and responses will be compulsory, with responses required to be timely.
Type of data that can be shared:	COSMIC participants (called "prescribed financial institutions") are entitled to share "risk information", which has been defined in the law broadly to mean, in relation to a relevant party of a prescribed financial institution, any of the following:[29] a) any particulars of the relevant party; b) any particulars of the relationship between the relevant party and the prescribed financial institution; c) any particulars of any transaction the relevant party is a party to; d) any particulars of the high-risk indicators in relation to the relevant party (that is, any behaviour of the relevant party, or any circumstance, that indicates a high risk that the relevant party may have been or may be concerned in money laundering, terrorism financing, or the financing of proliferation of weapons of mass destruction); e) the prescribed financial institution's analysis of high-risk indicators; f) any other information that the prescribed financial institution has obtained, or any other analysis that the prescribed financial institution has performed, for the purpose of assessing whether the relevant party may have been or may be concerned in money laundering, terrorism financing, or the financing of proliferation of weapons of mass destruction; g) any documents evidencing any of the matters in paragraphs (a) to (f); and h) any other information or documents that the Authority may prescribe.
Economic crime domain coverage:	COSMIC is initially focused on the following three key risks:[30] a) the misuse of legal persons, such as the abuse of shell companies, b) trade-based money laundering, and c) proliferation financing and the evasion of international sanctions. ECR coverage could be expanded to other AML/CFT threats under the relevant legislation, subject to authority of the Monetary Authority of Singapore (MAS). However, overall, COSMIC is only to be utilised for purposes of direct relevance to AML/CFT/CPF investigations. Singapore has alternative information sharing partnerships dedicated to the fraud and scams domain.

Type of entity that can participate:	Participation is limited to financial institutions. MAS plans to introduce COSMIC in phases. In the first phase, MAS has made COSMIC available to six major Singapore banks.[31] Subsequently, MAS plans to expand COSMIC's coverage to more focus areas and financial institutions and make sharing mandatory in higher-risk circumstances.[32]
Threshold for sharing and purpose limitations:	The Singapore COSMIC information sharing framework sets out three levels of collaboration, i.e. 'Request', 'Provide' and 'Alert'. 'Requests' are permissible when a customer has exhibited some red flag behaviour and a participant financial institution requires clarification from its counterpart financial institution on potential suspicion involving particular activity that the customer has exhibited. 'Provide' is a requirement when a customer's unusual activities cross a higher threshold, indicating a greater risk of the customer being involved in illicit activity. In this situation, a participant financial institution would have to proactively provide risk information on the customer to another participant financial institution with a link to the customer's activities. COSMIC 'Alerts' rely on a participant financial institution placing the customer on a watchlist to alert other participant financial institutions. An objective threshold, based on the number of red flags exhibited, needs to be crossed before information can be shared using any of the three modes. The thresholds are progressively higher for 'Request', 'Provide' and 'Alert'.[33]
Public sector involvement:	The Singapore COSMIC FISP is conceived as a public sector-led and managed initiative – though one which has been co-created between the public and private sector. MAS owns and operates COSMIC and integrates all COSMIC data into its own supervisory surveillance. In addition, the Suspicious Transaction Reporting Office, Singapore's FIU, has access to COSMIC information for its own analytics.[34]
Threat prioritisation process:	MAS sets clear threat priorities for the COSMIC partnership, as relevant to the priority risk areas identified in Singapore's National ML/TF Risk Assessment (as described above).
Cross-border element:	In Singapore, the COSMIC platform specifically acknowledges that financial institutions may need to disclose platform information for specific operational purposes, including "for group-wide ML/TF/PF risk management, and to facilitate the performance of ML/TF/PF risk management duties (e.g. for the carrying out of AML/CFT controls and processes including customer due diligence, transaction monitoring and AML data analytics, as well as audits on the financial institution's AML/CFT controls) and outsourcing of ML/TF/PF risk management operational functions."[35] (See more details below)

Distinctive features in the Singaporean P2P ECR collaboration regime include:

- **Public sector specificity in behaviour that will cross collaboration thresholds:** In COSMIC, an objective threshold needs to be crossed before information can be shared, with a different threshold trigger being relevant to each of the respective levels of information sharing 'Request', 'Provide' and 'Alert'. MAS will issue a directive to participant financial institutions detailing the threshold criteria for each of them, and the list of 'red flags' associated with each threshold. The red flags will correspond to known criminal profiles and behaviours for key financial crime risks. Only multiple red flags may trigger information sharing on COSMIC. The thresholds, details and permutations of the red flags must be kept strictly confidential among participant financial institutions to prevent criminals from circumventing them.[36]

- **Cross-border element:** COSMIC permits sharing of information that financial institutions receive from COSMIC to both their local and overseas affiliates, only for group-wide ML/TF/PF risk management purposes, on a need-to-know basis and provided that additional conditions are met. Financial institutions are required to comply with additional safeguards when sharing to individuals outside of Singapore.[37]

- **Safeguards to protect legitimate customers:** There are safeguards in place to protect legitimate customers inadvertently associated with bad actors, such as those who unknowingly trade with an illicit counterparty. Participant financial institutions should first assess if there are valid reasons for the customer's behaviour or profile before sharing information on COSMIC. Banks, as part of their risk assessment, are also expected to reach out to customers to allow them the opportunity to address the bank's risk concerns and to explain unusual behaviours observed.

- **Direct communication with suspects**: Singapore COSMIC member financial institutions, in their risk assessment around a client exit procedure, cannot rely solely on information from COSMIC when making a decision, but must consider other relevant information that might be available. This may include a financial institution's investigations or other external sources (such as clarifications from the customer). [38] Financial institutions may contact the customer and provide them with "adequate opportunity to explain the observed activity", subject to the 'no tipping-off' requirement.[39]

- **Criminal penalties for members' misuse of the facility**: The Singapore COSMIC platform imposes a number of legal duties on participant financial institutions.

  Duties on participant financial institutions:[40]

  a) Ensure that information disclosed on the platform is accurate and complete, promptly notify MAS and other relevant participant financial institutions of any error in the information provided, and rectify such errors as soon as possible; and
  b) establish and implement systems and processes to safeguard the information disclosed and received.

  While initiating requests for information through COSMIC is currently voluntary for participant financial institutions, responses are mandatory. MAS is considering making the initiation of 'provide' and 'alert' messages mandatory for higher-risk cases in the future. Participant financial institutions may be subject to penalties if they fail to comply with the above requirements.

iv. UK

UK

Legislative reference and enactment date:	The Economic Crime and Corporate Transparency Act 2023 (ECCTA) measures for AML information sharing came into force on the 15 January 2024, meaning obliged entities have been able to share under these provisions since that date. ECCTA sections 188 and 189 provide for civil liability to be disapplied related to the information sharing; subject to the information sharing process, threshold and participants meeting the necessary conditions. ECCTA involves two scenarios of P2P information sharing: a bi-lateral 'request' for information and a 'warning' capability (one-to-many) which can be carried out through a third-party intermediary. In terms of the legal provisions, "direct sharing" under s188 enables bi-lateral communication and can support both the 'request' and the 'warning' capabilities. 'Indirect sharing' under s189, through a third-party intermediary, only supports the 'warning' capability: 1. **Direct sharing of information with another obliged entity in the AML regulated sector (s188):** Bi-lateral 'direct sharing' provisions enable obliged entities to share customer information with each other with civil liability disapplied on a peer-to-peer basis. 2. **Indirect sharing of information via a third-party intermediary (s189):** Multi-lateral 'indirect sharing' provisions enable a smaller subset of applicable obliged entities to share a third-party intermediary. Third party intermediaries may include existing or new sector specific and cross sector economic crime consortia. These intermediary organisations may be able to provide analysis on the customer information being shared, to provide obliged entities with enriched data sources. Indirect sharing can relate only to a 'warning', i.e. a 'request' is not permitted through indirect sharing/s189. The UK ECCTA is not the only legislation relevant to ECR information sharing and the UK has a broad tapestry of fraud-risk information sharing enabled through GDPR (described in the FFIS 2022 survey[41]) and opportunities to share risk information without the disapplication of civil liability provided by ECCTA. The following analysis refers to the ECCTA only.
Compulsory or voluntary:	ECCTA information sharing is voluntary.
Type of data that can be shared:	Information will relate to 'customer information'. There is no definition of the 'customer information' and it is intended by policy-makers that obliged entities decide which data they will want to share. However, the Government's Impact Assessment[42] indicates that 'customer information' would include such information that may assist the recipient obliged entity in deciding:

	• whether the veracity of documents should be doubted (such as identity verification); • whether due diligence is required in relation to an existing customer; • whether a particular case or customer carries a high risk of economic crime; and/or • the extent of the measures that should be taken to manage or mitigate that risk. Information that can be shared relates to existing or past customers only.
Economic crime domain coverage:	Information shared must be for the purposes of preventing, investigating or detecting "economic crime". Economic crime in this context includes money laundering, terrorist financing, bribery, sanctions evasion, tax evasion, market abuse and fraud. It also includes inchoate offences such as attempt or conspiracy (Inchoate offences are crimes that occur when a defendant takes steps towards committing a crime but does not actually commit it).[43]
Type of entity that can participate:	Section 188 'direct sharing' can take place between any AML obliged entities in the UK. Section 189 'indirect sharing', i.e. sharing through a third-party intermediary for businesses in the financial sector, can take place between deposit-taking bodies, electronic money institutions and payment institutions, cryptoasset exchanges and custodian wallet providers, large law firms, large accountancy firms, large insolvency practitioners, large auditors and large tax advisers. Large firms are defined, in line with the UK Economic Crime Levy legislation, as those having revenues of between £36 million and £1 billion.
Threshold for sharing and purpose limitations:	Participating obliged entities receive protection against a breach of confidence or other civil liability if the disclosure is made for the purposes of preventing economic crime. Obliged entities must use the request and/or the warning conditions set out in the legislation to receive protection. Under the request condition, one obliged entity can request customer information from another obliged entity if they believe that the organisation they request information from holds information relating to a customer that will or may assist the requesting obliged entity in carrying out relevant AML/CFT actions. For the 'warning' scenario, the threshold is met when an obliged entity has taken 'safeguarding action' or would have done so had the customer remained onboarded. Safeguarding action means: "terminating a business relationship with the customer, refusing the customer a product or service, or restricting the customer's access to elements of a product or service made available to other customers. A business relationship in this context means one that arises out of the firm's business and is expected to have an element of duration."[44]
Public sector involvement:	These provisions do not include law enforcement involvement. A key element of the ECCTA proposals (advancing on the UK Criminal Finances Act 2017 provisions for information sharing) is that there is no need to notify the UK National Crime Agency during the ECCTA information sharing process and an obliged entity can share information with another obliged entity about a customer without having been prompted to do so by that other obliged entity.

	As such, the provisions are conceived very much as a P2P collaboration framework and not a PPP legal authority. UK public-private partnership sharing occurs, in the AML regime, through the section 7 legal gateway of the Crime and Courts Act 2015 and is hosted in practice by the JMLIT+ public private partnership through the National Crime Agency.
Threat prioritisation process:	ECCTA sharing does not come with any inherent prioritisation and is left to the private sector to implement. However, in line with the 'UK Economic Crime Plan 2023-26',[45] the UK Home Office and UK Finance are developing a system to link regulatory expectations on obliged entities to respond to national intelligence priorities. If completed, this prioritisation framework would likely have an impact on ECCTA collaboration and the priorities adopted by ECCTA P2P participants.
Cross-border element:	No. These new measures are domestic in their application. In practice, this means that the disapplication of civil liability in the legislation is limited to UK-based information sharing, and this would not apply to sharing outside of the UK.[46]

Distinctive features in the UK ECCTA collaboration regime include:

- **Two specific use case scenarios authorised by the P2P legislation:** The October 2024 UK Guidance on ECCTA information sharing specified the following:[47]

  "Under the request condition, one firm can request customer information from another firm on the basis that they believe that the organisation sharing holds information, relating to a customer, that will or may assist the requesting firm in carrying out relevant actions. Relevant actions refer to a firm deciding whether it is appropriate to apply due diligence, undertaking effective measures for verifying the identity of the customer or determining whether it is appropriate to terminate an existing business relationship with a customer… the warning condition involves a firm sharing information with another firm about a customer without having been prompted by that other firm … In practice, this would mean that applicable firms would only be able to upload customer information on an individual onto a third-party sharing database, if they had decided to take safeguarding action."

- **Policy leadership about maximising the use of the provision and expected outcomes:** The UK government wants to maximise lawful information sharing under the provision, clarifying that "The government encourages the use of both direct and indirect sharing under the new provisions to prevent, investigate and detect economic crime."[48] The UK set out policy objectives for the outcomes of ECCTA sharing in the October 2024 Guidance as: "regulated firms using the measures to share information… will gain a network view of the economic crime risk linked to their services and platforms. Firms will therefore have a greater ability to take upstream preventative action and disrupt illicit activity" (Paragraph 8) and to "increase the accuracy of suspicious activity and fraud reporting" (Paragraph 9) and "the government therefore supports cross-sector sharing under these new measures, including via direct and indirect sharing mechanisms." (Paragraph 44)

- **Clarity on third-party analytics:** The October 2024 guidance also clarified "Regulated firms who are also in scope of the indirect sharing provisions can share both on a peer-to-peer basis and through a third-party intermediary. Third-party intermediaries may include existing or new sector specific and cross sector economic crime consortia. These intermediary organisations may be able to provide analysis on the customer information being shared, to provide regulated firms with enriched data sources."[49]

v. EU

The EU

Legislative reference and enactment date:	The EU AML Regulation[50] (AMLR) was adopted by the EU co-legislators (the European Parliament and the Council of the EU) on 31 May 2024. The AMLR will be directly applicable from 10 July 2027. Article 75 lays down the rules for the exchange of information in the framework of partnerships for information sharing. Another legislative instrument, the EU AML Authority (AMLA) Regulation, provides the future Authority with the possibility to set up cross-border partnerships for information sharing and participate in such partnerships. Relevant data can only be shared in a ***verified*** Article 75 partnership structure, i.e. one that has been verified by the AML supervisor prior to collaboration taking place. There is no prescriptive requirement regarding the legal form that the partnership should take.
Compulsory or voluntary:	Information sharing on the basis of AMLR Article 75 is voluntary.
Type of data that can be shared:	The EU AMLR Article 75 clearly sets out the information which can be shared, as: a) information on the customer, including any information obtained in the course of identifying and verifying the identity of the customer and, where relevant, the beneficial owner of the customer; b) information on the purpose and intended nature of the business relationship or occasional transaction between the customer and the obliged entity, as well as, where applicable, the source of wealth and source of funds of the customer; c) information on customer transactions; d) information on higher and lower risk factors associated with the customer; e) the obliged entity's analysis of the risks associated with the customer pursuant to [Customer due diligence measures] Article 20(2); f) information held by the obliged entity pursuant to [Record retention obligations] Article 77(1); and g) information on suspicions pursuant to [Reporting of suspicions article] Article 69.
Economic crime domain coverage:	Article 75 is set within the AML framework and includes domains of: • Money laundering; • Predicate offences (therefore including fraud and corruption, for example); and • Terrorist financing.
Type of entity that can participate:	Any obliged entity under the EU's AML/CFT regime can participate in a partnership for information sharing established under Article 75 of the AMLR. As such, membership of a partnership can include multiple types of financial and credit institutions as well as non-financial sector entities (e.g., notaries, accountants, real estate agents, trust or

	company service providers, providers of gambling services). Both sector-specific partnerships and cross-sector sharing is possible. There is no limitation to the partnerships that can be set up within an EU Member State (national or cross-border), nor to the number of partnerships that an obliged entity can participate in.
Threshold for sharing and purpose limitations:	Paragraph 1 of Article 75 emphasises that "Members of partnerships for information sharing may share information among each other where strictly necessary for the purposes of complying with the obligations under Chapter III [customer due diligence] and Article 69 [reporting of suspicions] and in accordance with fundamental rights and judicial procedural safeguards." Paragraph 4(f) of Article 75 sets out a threshold for information sharing based on customer activity, such that "the sharing of information shall be carried out only in relation to customers: i. whose behaviour or transaction activities are associated with a higher risk of money laundering, its predicate offences or terrorist financing, as identified pursuant to the risk assessment at Union level and the national risk assessment; ii. who fall under any of the situations referred to in Articles 29, 30, 31 and 36 to 46 of this Regulation;[51] or iii. for whom the obliged entities need to collect additional information in order to determine whether they are associated with a higher level of risk of money laundering, its predicate offences or terrorist financing.
Public sector involvement:	Yes. The AMLR Article 75 permits competent authorities (AML/CFT supervisors, FIUs and authorities having the function to investigate or prosecute money laundering, its predicate offences or terrorist financing, or the function of tracing, seizing or freezing and confiscating criminal assets) to participate in a partnership for information sharing. Article 75 sets out that "the competent authorities that are members of a partnership for information sharing shall only obtain, provide and exchange information to the extent that this is necessary for the performance of their tasks under relevant Union or national law". These tasks could include, e.g., AML/CFT supervision, analysis of suspicious transactions and activities by FIUs and information sharing with counterparts from other Member States. The authorities competent for the investigation and prosecution of money launderings, its predicate offences or terrorist financing and/or for the tracing, seizing or freezing and confiscation of criminal assets that take part in an information sharing partnership shall obtain, provide or exchange personal data and operational information in accordance with national law.[52] In this way criminal law investigative authorities **can** share information within a partnership, subject to being able to make use of additional (national-level) enabling legislation for the information sharing between that agency and the members of the Article 75 partnership.
Threat prioritisation process:	Article 75 partnership threat prioritisation is tied to the risk assessment priorities of the European Union and at the national level, as set out in Article 75 paragraph 4(f) (quoted above).

Cross-border element:	There is no prohibition on cross-border Article 75 partnerships (across national borders, intra-EU) and indeed information from a partnership can be shared with the EU's AML Authority (EU AMLA). Under Article 93 of the AMLA Regulation, AMLA also has the mandate to set up cross-border partnerships for information sharing and participate in partnerships established in one or across several Member States with the objective of supporting the prevention and combating of money laundering, its predicate offences and terrorist financing. Information sharing outside of the EU is not permitted by Article 75 of the AMLR.

There are a number of distinctive features in the EU's P2P ECR collaboration regime, including:

- **The paragraph 4 conditions:** The EU's regime is arguably the most detailed in terms of setting out the specific conditions that an Article 75 partnership must comply with; relating to data protection as well as measures to safeguard the rights of affected persons and legitimate customers.

- **Cross-border information sharing:** The new EU regime supports cross-border AML information sharing partnerships (within the EU) through the interaction described above between Article 75 of the AMLR and Article 93 of the AMLA Regulation.

- **Verification:** Obliged entities intending to set up a partnership for information sharing must notify their respective AML supervisory authorities who have a new duty to verify the compliance of the partnership with the Article 75 conditions, prior to information sharing taking place. This represents something of a 'safety net' for Article 75 partnership designers who might otherwise be left with a greater risk that their partnership design was out of line with the expectations of supervisors and therefore vulnerable to supervisory enforcement action by either the AML supervisor or data protection authority. This 'Paragraph 2' verification process is expected to stimulate cross-agency dialogue between AML supervisors, data protection authorities and FIUs about the appropriate use of Article 75.

- **Link with privacy enhancing technologies (PETs):** Article 75 is the only AML collaboration legal framework that makes explicit reference to the importance of pseudonymisation. Paragraph 4 (e) sets out that "obliged entities shall implement appropriate technical and organisational measures, including measures to allow pseudonymisation, to ensure a level of security and confidentiality proportionate to the nature and extent of the information exchanged". This may provide a spur for the use of PETs to enable the sharing of insight without the sharing of the raw data.

vi. Canada

Canada

Legislative reference and enactment date:	Canadian (Federal Law) Section 11.01 Amendments to the Proceeds of Crime and (Money Laundering) and Terrorist Financing Act (PCMLTFA) (2000, updated in 2024), with amendments enacted through Bill C-69 - Government Bill (House of Commons) C-69 (44-1) - Royal Assent - Budget Implementation Act, 2024, No. 1 - Parliament of Canada. This legislation essentially provides an exception to the 'PIPEDA' privacy statute obligation on federally regulated private sector entities to seek consent when sharing personal information. Regulations are due to accompany this legislation to set out the full conditions, requirements, and standards that obliged entities must satisfy to make use of this provision.[53]
Compulsory or voluntary:	Information sharing through Section 11.01 is voluntary and responses are also voluntary.
Type of data that can be shared:	No restrictions on data types are identified in the legislation.
Economic crime domain coverage:	Money laundering, terrorist activity financing and sanctions evasion are the stated threats, with money muling of stolen funds (fraud) also in scope.
Type of entity that can participate:	All regulated entities under the Canadian AML/ATF regime (described in Part 1, Section 5 of the Proceeds of Crime and (Money Laundering) and Terrorist Financing Act).
Threshold for sharing and purpose limitations:	Such sharing is permitted if the disclosure is "reasonable for the purpose of detecting or deterring money laundering, terrorist activity financing or sanctions evasion." (11.01 (1) (b))
Public sector involvement:	Not authorised within 11.01.
Threat prioritisation process:	There is no inherent threat prioritisation within 11.01.
Cross-border element:	There is no specific enabling feature within 11.01 to share information across borders.

Distinctive features in the Canadian 11.01 P2P ECR collaboration regime include:

- **Protection from civil and criminal liability for the use of the information.** Section 11.01, 'Disclosure without consent', provides an exception to Canadian privacy law obligations that, otherwise, would require federally-regulated private sector entities to seek consent for certain acts of information sharing. Section 11.01 provides obliged entities with protections from criminal and civil liability for information sharing ("safe harbor"), subject to the exception being implemented in line with its intended purposes.

- **Codes of Practice.** Prior to making use of the 11.01 exception, obliged entities are required to develop a Code of Practice, which sets out: the participants of the information sharing partnership; the intended use of the information to be exchanged; the type of information to be exchanged; how information would be exchanged; how the information would be stored/records kept; and an explanation of the consistency of the information sharing with the exception. Codes of Practice are intended to be principles-based to allow for different uses under different scenarios.

- **Public sector pre-sharing approvals process.** Similar to the paragraph 2 'verification' process under the EU's AMLR Article 75, under the 11.01 exception FINTRAC (the Canadian FIU and AML supervisor) and the Canadian Office of the Privacy Commissioner (OPC) have distinct roles in pre-sharing approval. Whereas in the EU, *the AML supervisor* must 'verify' the partnership; in Canada, the OPC – as *the data protection authority* – has a similar role. The OPC must approve any Code of Practice prior to information sharing taking place. FINTRAC may provide comments to the OPC and/or the obliged entities as part of this process. Obliged entities are not able to make use of the 11.01 exception until the OPC approval process is complete. Minor changes to the code must be notified to the OPC and FINTRAC, while material changes to the code would recommence OPC approval processes.

- **Privacy Commissioner assessment of the code.** The OPC will approve the Code of Practice if they determine that the code meets the criteria set out in the regulations. The Commissioner must be satisfied that the code sufficiently explains how it will provide for substantially the same or greater protection of personal information as is provided under PIPEDA, other than as allowed by the PCMLTFA exception. The Commissioner will have a prescribed period of 90 days, extendable by 15 days, to review the code and provide either its written approval or written deficiencies. After approval, the Commissioner may, with cause, direct that the code be resubmitted for approval.

- **FINTRAC assessment of the code.** FINTRAC has an opportunity to provide comments to the OPC and/or obliged entities relevant to a proposed Code of Practice. Once approved by the OPC, FINTRAC takes on new supervision responsibility to ensure the code of practice is in place prior to the sharing of relevant information and that the parameters specified in the code are adhered to by obliged/reporting entities.

1.3. Comparing legislative frameworks for ECR collaboration

Table 2. P2P legal frameworks quick reference table

Key variables in the legislation	USA 314(b)	Mexico LIC Article 115 Bis	Singapore (COSMIC)	UK ECCTA S188 and S189	EU AMLR Article 75	Canada 11.01 Exception
Threshold for lawful information sharing:	No explicit threshold or trigger conditions set in law.	An alert in at least one bank.	Alerts, related to defined 'red-flags' enable the first level of information sharing 'requests'.	Having 'taken safeguarding action' for indirect sharing.	'Strict necessity' and meeting the paragraph 4(f) threshold conditions for customer activity.	Sharing must be reasonable and subject to a code of practice.
Membership:						
All financial institutions can participate?		[3]	[4]			
All AML-obliged entities can participate?	[5]	[6]	[7]	[8]		
Cross-sector sharing is possible?	[9]	[10]	[11]	[12]		
The P2P law enables LEA/FIU participation?[13]	[14]	[15]		[16]	[17]	[18]
Other legal provisions allow operational PPP?[19]	[20]	[21]		[22]	[23]	[24]
Other P2P features:						
Cross-border sharing enabled by the P2P law?	[25]	[26]	[27]	[28]	[29]	[30]
P2P sharing is supported by AML supervision?[31]	[32]	[33]	[34]	[35]	[36]	[37]
P2P network-level 'consortium' analysis possible?[38]		[39]	[40]	[41]	[42]	[43]

Legend

Condition not met	Condition partially met	Condition met

Table notes:

[3] Article 115 Bis establishes an information sharing authority only for banks

[4] As a design choice, in the current phase, MAS has made COSMIC available only to six major Singapore banks.

[5] 314(b) associations for multi-party information sharing are only open to financial institutions as participants.

[6] Only financial institutions can participate in LIC 115 Bis sharing or 62nd Ter of the AML/CFT Rules cross-border sharing.

[7] As a design choice, in the current phase, MAS has made COSMIC available only to six major Singapore banks.

[8] ECCTA S188 is available to all obliged entities (for direct sharing), but S189 indirect multi-party sharing is only for a subset of obliged entities

[9] 314(b) associations for multi-party information sharing are only available to financial institutions to join.

[10] Only financial institutions can participate in LIC Article 115 Bis sharing or 62nd Ter - Octies of the AML/CFT Rules cross-border sharing.

[11] As a design choice, in the current phase, MAS has made COSMIC available only to six major Singapore banks.

[12] While ECCTA S188 is available to all obliged entities (for direct sharing), and S189 indirect multi-party sharing is only for a subset of obliged entities, under both provisions cross-sector sharing is possible.

[13] This condition relates to whether the respective P2P law also legislates for law enforcement or financial intelligence unit public sector engagement in the information-sharing partnerships.

[14] Information-sharing by public authorities, such as law enforcement authorities, is not legislated for within 314(b).

[15] Information-sharing by public authorities, such as law enforcement authorities, is not legislated for within LIC Article 115 Bis or the AML/CFT Rules.

[16] Information-sharing by public authorities, such as law enforcement authorities, is not legislated for within ECCTA S188 or 189.

[17] Article 75 provides no additional legal basis for Information-sharing by public authorities, such as law enforcement authorities or criminal law investigative authorities, to share information. However, it does leave open the potential for authorities competent for the investigation and prosecution of money launderings, its predicate offences or terrorist financing and/or for the tracing, seizing or freezing and confiscation of criminal assets that take part in an information sharing partnership, only in accordance with relevant national law. Article 75 provides additional safeguards on the competent authorities that are members of a partnership for information sharing in that such authorities "shall only obtain, provide and exchange information to the extent that this is necessary for the performance of their tasks under relevant Union or national law".

[18] Information-sharing by public authorities, such as law enforcement authorities, is not legislated for within the 11.01 exception.

[19] This condition relates to whether – beyond the respective P2P law – other legal provisions in that a country or jurisdiction allow for separate 'operational' AML/CTF public-private information-sharing, permitting law enforcement or financial intelligence unit public sector direct information sharing of personal data with obliged entities relevant to criminal law investigations

[20] public agencies use 314(a) of the PATRIOT Act to facilitate information exchange from competent authorities or other legislative gateways may be used by law enforcement to share information with the private sector.

[21] As far as this author could determine, there are no PPPs in Mexico sharing operational case-sensitive personal data between criminal law investigative authorities and private sector obliged entities in the AML/CTF domain.

[22] UK public-private partnership information sharing occurs, in the AML regime, through the section 7 legal gateway of the Crime and Courts Act 2015 and is hosted in practice by the JMLIT+ public private partnership through the National Crime Agency /National Economic Crime Centre (NECC).

[23] Criminal law investigative authorities can be members of an Article 75 partnership, but only subject to additional national law establishing such a legal gateway.

[24] As far as this author could determine, there are no PPPs in Canada sharing operational case-sensitive personal data between criminal law investigative authorities and private sector obliged entities in the AML/CTF domain

[25] 314(b) does not provide 'safe harbour' for cross-border sharing, but no law in the U.S. prohibits such sharing and the AML supervisor actively encourages forms of such sharing.

[26] Pursuant to the 62nd Ter of the AML/CFT Rules, Mexican banks may exchange information of their customers' and users' operations with similar Foreign Financial Entities, solely and exclusively for the purpose of strengthening the AML/CFT measures with Foreign Financial Entities (EFEs).

[27] COSMIC permits such sharing of information that financial institutions receive from COSMIC to both their local and overseas affiliates, only for group-wide ML/TF/PF risk management purposes, on a need-to-know basis and provided that additional conditions are met. Financial institutions are required to comply with additional safeguards when sharing to individuals outside of Singapore.

[28] ECCTA sharing is domestic only in application to the UK.

[29] Cross-border sharing intra-EU is permitted, but such sharing is not permitted outside of the EU.

[30] Section 11.01 exceptions are for domestic application in Canada only.

[31] Meaning that the use of the P2P legislative gateway is actively encouraged by the AML supervisor.

[32] U.S. AMLA requires that supervisors take note of value to law enforcement in an examination and the AML supervisor has expressed the priority it places on private-to-private information sharing.

[33] In Mexico, there are no specific consequences for AML supervision arising from an obliged entity's participation or non-participation in a P2P collaboration. However, the AML supervisor is responsible for assessing compliance with the conditions of information-sharing.

[34] In Singapore, COSMIC use is promoted by the AML supervisor and the COSMIC framework requires compulsory responses to requests. While there are currently no consequences in terms of AML supervision arising from participation or non-participation in COSMIC collaboration, COSMIC participation (for the target members) is intended by the AML supervisor to become compulsory in the future. In the meantime, COSMIC participants must abide by clear rules set out in primary legislation and MAS' COSMIC Notice, to ensure that, inter alia, sharing is only for legitimate AML/CFT purposes and subject to robust safeguards. MAS also takes into account FIs' contributions to detecting and combating ML/TF cases and law enforcement agencies' feedback of such contribution in our supervision, albeit this is not confined just to COSMIC-related cases.

[35] In the UK, there are no specific consequences for AML supervision arising from an obliged entity's participation or non-participation in a P2P collaboration.

[36] In the EU, there are no specific consequences for AML supervision arising from an obliged entity's participation or non-participation in a P2P collaboration.

[37] FINTRAC takes on new duties of supervising that partnership members have an approved code of practice in place before participating, but it remains to be seen as whether FINTRAC actively encourages obliged entities to participate in such partnerships or the results and impact of such sharing are relevant in the course of AML supervisory inspections.

[38] This condition refers to whether the multi-party P2P platforms can achieve a network-level view of risk, beyond what members can see themselves and analyse and communicate that risk to members.

[39] The extent of network level analysis permitted by the legislation is not yet clear or has not been explicitly supported yet in public sector guidance.

[40] The COSMIC 'request', 'provide' or 'alert' functionality does not envisage new risk being communicated to members that at least one member has not already observed. However, Singaporean public authorities may be able to leverage data insights from COSMIC and proactively provide such new insights on risk to members.

[41] In the UK, October 2024 guidance described in the previous section clarifies that a third party analytical hub can enrich data shared by members and provide additional financial crime insights.

[42] The extent of network level analysis permitted by the legislation is not yet clear or has not been explicitly supported yet in public sector guidance.

[43] The extent of network level analysis permitted by the legislation is not yet clear or has not been explicitly supported yet in public sector guidance.

Interesting points of distinction from the across the U.S., Mexico, Singapore, UK, EU and Canadian legislative frameworks include:

The range of entities that can participate in the information sharing:

The range of entities that can engage in the information sharing varies from just financial institutions, through to all obliged entities, to even beyond AML-obliged entities.

Smaller range of business sectors can participate			**A larger range of sectors**
Singapore and Mexico	**U.S.**	**UK**	**EU and Canada**
Only financial institutions can engage in the information sharing. In Singapore, only six banks are currently able to participate in COSMIC.	While all obliged entities under the Banking Secrecy Act can register for 314(b), only financial institutions can engage in multi-party information sharing through 314(b) associations.	All AML obliged entities can share directly (S188). However, the types of regulated firms that can share indirectly through a third-party intermediary are a smaller sub-set of the wider regulated sector (but beyond just financial institutions) (S189).	All obliged entities can engage in the P2P information sharing regime.

The threshold for sharing

The threshold for when sharing can take place varies across the different legislative frameworks. This threshold has a major impact on the models of information sharing that can be implemented and the type of collaborative analytics capability that is possible. Across the U.S., Mexico, Singapore, the UK, the EU and Canada, the threshold for sharing varies from requiring 'safeguarding action to be taken' by an obliged entity prior to sharing (UK), to a broader language related to sharing information that could help determine whether a customer is 'higher' risk (EU), to relying on specific indicators that are published by the government (Singapore), to to whether sharing is reasonable and subject to a code of practice (Canada), and to where there is no threshold or trigger set of conditions indicated in law (the U.S. and Mexico).

Higher threshold before sharing can take place			**Lower threshold**
UK	**EU**	**Singapore**	**U.S., Mexico and Canada**
The UK requires that 'safeguarding action' be taken on the customer as a pre-requisite for 'indirect sharing' (S189).[44]	Article 75 emphasises the requirement to meet a standard of 'strict necessity' and sets out additional threshold conditions in 4(f), which permit information sharing in order to 'determine higher risk'.	The Monetary Authority of Singapore publishes specific risk indicators that set the first bar for information sharing.	The U.S. and Mexico do not place an explicit threshold condition for information sharing, but an alert is generally considered to be required. In Canada, the test is one of 'reasonableness' in line with the purpose and subject to a code of practice.

[44] Though it should be noted that the threshold for UK (S188) 'direct sharing' bi-lateral messaging is much lower – covered by the 4th October 2024 Guidance under the 'Request condition'; i.e. "Under the request condition, one firm can request customer information from another firm on the basis that they believe that the organisation sharing holds information, relating to a customer, that will or may assist the requesting firm in carrying out relevant actions." https://www.gov.uk/government/publications/information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act/guidance-on-the-information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act-2023

In addition, we note the following characteristics which differentiate the legal frameworks:

Table 3. Notes on variance between the P2P legislative environments on additional factors

Factor	Notes on variance between the legislative environments
Non-customer risk data	Under the six legislative regimes analysed, there is generally quite a wide range of data that can be shared about customers. A key point of distinction is whether risk information about counterparty non-customers (i.e. risk related to *recipients* of payments who are **not customers** of that financial institution) can be shared. This appears not to be permissible in the Mexico, EU and UK frameworks, but permissible in the U.S., Singapore and Canadian frameworks.
Public sector authority observer visibility of the information shared	Aside from the question of whether a public agency is an active member of a partnership, countries vary as to whether relevant public authorities have an observer capacity for AML P2P collaboration, i.e. whether public authorities have visibility of the underlying information shared within P2P partnerships. In the Singapore framework, both the Monetary Authority of Singapore and the Singapore Financial Intelligence Unit have the ability to analyse all of the information shared by participant financial institutions. In the UK and U.S., information sharing has been designed to ensure that such P2P sharing is **not** visible to public agencies prior to the filing of a Suspicious Activity Report. In Mexico, public authorities have observer visibility for cross-border information sharing elements only. In the EU, there is no public sector observer visibility of the information shared, apart from in the case that information relates to a Suspicious Activity (or Transaction) Report (in which case the relevant FIU must agree to the disclosure).
Threat prioritisation process	The collaboration frameworks vary in terms of the threat prioritisation: from specific (government-directed) use-cases (Singapore), to an emphasis on national or EU risk assessment priorities (EU), to a link to national priorities (USA), to no particular threat priorities described within the statute (Canada, the UK and Mexico).
Cross-border element	The extent of cross-border information sharing enabled by the respective AML collaboration frameworks varies: from supporting intra EU cross-border information sharing partnerships (EU), to legal provisions that enable cross-border information sharing (Mexico and Singapore), to having no clear link to cross-border information sharing (UK, US and Canada).

1.4. The different legislative frameworks promote different AML collaborative capabilities

A key, if not central, point of distinction between the legislative frameworks is to determine what information sharing capabilities or models they support.

The FFIS (2022) survey[54] included a taxonomy of major types of private-to-private sharing capabilities. Below we analyse the six legislative frameworks against an expanded list of private-to-private sharing capabilities (differentiating between bi-lateral and multi-party messaging communication in an updated taxonomy):

A.	Data-driven collaborative development of typologies of economic crime threats.
B.i.	Messaging communication (bi-lateral).
B.ii.	Messaging communication (multiparty and via a platform).
C.	Intelligence development at the level of a multi-party platform, to identify risk that no individual participant had otherwise observed.
D.i.	Joint case investigations by members (private sector only).
D.ii.	Collaborative intelligence and joint investigations by members (with law enforcement or investigative agency input).
E.	A warning function, one to many (i.e. an adverse incident database).
F.	A tracing function to identify exposure to money laundering/muling dispersals (i.e. a rapid or automated warning chains of alerts to follow transactions across multiple obliged entities, illuminating the network of accounts involved in a dispersal).
G.	Combined transaction monitoring for partnership members.

See FFIS (2022) "Lessons in private-to-private financial information sharing to detect and disrupt crime", A Survey and Policy Discussion Paper for analysis of the strengths, shortcomings and different data dependencies for each capability and the FATF Guidance "Private Sector Information Sharing" (2017), which originally described a range of benefits associated to private sector information sharing models.

Drawing from the legal texts and FFIS discussion events on the scope of the respective legal gateways, the table below indicates how the legislative environments support different ECR collaboration capabilities. The table is a FFIS assessment following the comparative review of the legislation. The assessment is not a legal opinion and has no legal authority. Interpretations of the legislation are subject to change and evolution in legal understanding, with the issuance of new guidance and through case-law over time.

Table 4. P2P frameworks compared in terms of the permissibility of ECR collaboration capabilities

ECR collaboration capability		 USA 314(b)	 Mexico LIC Article 115 Bis	 Singapore (COSMIC)	 UK ECCTA S188 and S189	 EU AMLR Article 75	 Canada 11.01 Exception
A.	Data-driven collaborative development of typologies of economic crime threats	✓ Assessed to be possible under 314(b).	— Not an explicit feature of the Article 115 Bis enabling framework, but possible if no personal data is shared.	— Not an explicit feature of the COSMIC enabling framework, but possible if no personal data is shared.	— Not an explicit feature of the ECCTA enabling framework, but possible if no personal data is shared.	✓ Assessed to be possible, subject to paragraph 4(f) threshold conditions.	✓ Assessed to be possible under the 11.01 exception, even if personal information is shared, subject to the conditions being met.
B.i.	Messaging communication (bi-lateral)	✓ Yes. This is a traditional use-case for 314(b).	✓ Yes. This is the original use-case envisaged in the legislation.	✓ Yes. The 'request' or the 'provide' functionality support bilateral sharing.	✓ Yes. This is the focus of the S188 'direct sharing' legal gateway.	✓ Yes. This form of communication represents the most targeted form of sharing and the most limited dispersal.	✓ Yes. This form of communication represents the most targeted form of sharing and the most limited dispersal.
B.ii.	Messaging communication (multiparty and via a platform)	✓ Yes. This use of 314(b) has accelerated through '314(b) associations' since 2015 in particular.	✓ Yes, a 2022 clarification from Mexican authorities confirmed this was authorised.	✓ Yes. The COSMIC 'alert' sharing is multiparty.	✗ While multi-party information sharing through a platform is permitted in S189, the 'request' capability is not permitted under S189 (only the 'warning' capability is permitted through S189).	✓ Yes, subject to all of the members of the platform for information sharing meeting the Article 75 conditions.	✓ Yes. This form of communication is expected to be possible.
C.	Intelligence development at the level of a multi-party platform, to identify risk that no individual participant had otherwise observed	✓ Yes. '314(b) associations' are permitted to proactively identify financial crime and fraud risk leveraging the collective data of their members.	— It is unclear whether a platform for information sharing in Mexico Article 115 Bis can derive new financial crime insights and share those with members, beyond what has already been shared by at least one participant member.	— The COSMIC 'request', 'provide' or 'alert' functionality does not envisage new risk being communicated to members that at least one member has not already observed. However, Singaporean public authorities may be able to leverage data insights from COSMIC and proactively provide such new insights on risk to members.	— It is unclear whether a platform for information sharing under S189 can derive new financial crime insights and share that intelligence with members, beyond what has already been shared by at least one participant member.	— It is unclear whether a platform for information sharing under Article 75 can derive new financial crime insights and share those with members, beyond what has already been shared by at least one participant member.	— It is unclear whether a platform for information sharing under the 11.01 exception can derive new financial crime insights and share those with members, beyond what has already been shared by at least one participant member.
D.i.	Joint case investigations by members **(private sector only)**	✓ Yes. This use of 314(b) has accelerated through consortium models and within some 314(b) associations.	✓ This feature is possible within the new Article 115 Bis regime	✗ This is not a design feature of COSMIC.	— This use-case is not permissible under S189, but it permissible under the UK Criminal Finances Act 2019 powers.	✓ Yes, subject to paragraph 4(f) threshold conditions being met.	✓ Yes. This form of collaboration on joint development of cases is expected to be possible.

D.ii.	Collaborative intelligence and joint investigations by members **(with law enforcement or investigative agency input)**	314(b) is for private sector collaboration only, but with the connection to 314(a) of the USA PATRIOT Act or other mechanisms for law enforcement sharing, law enforcement investigative insight can be connected to a consortium.	Article 115 Bis is for private sector sharing only and there is no parallel legislation to support law enforcement input to a P2P platform.	This is not a design feature of COSMIC. However, the Singapore 'ACIP' PPP provides a space for such a use-case.	Law enforcement input is not a feature of the ECCTA sharing legislative gateway for information sharing. An alternative legal gateway in the UK allows for this capability (Section 7 of the Crime and Courts Act 2015 through the National Crime Agency-led JMLIT+ PPP framework).	Not a feature permitted by Article 75 by itself. Law enforcement input would be possible to an Article 75 partnership in situations where law enforcement or criminal law investigative entities are permitted to share the relevant information to the private sector in accordance with national law.	The Canada 11.01 exception is relevant for private-to-private information sharing and does not provide any additional authorities for law enforcement or investigative agency input into an 11.01 partnership.
E.	A warning function, one to many (i.e. an adverse incident database)	This is not a traditional use of 314(b) in terms of sharing the reasons for AML client exit decisions, though confirmed fraud incidents and other risk information can be shared through 314(b) associations.	Assessed to be possible, but it remains to be developed in practice in an Article 115 Bis platform. However, this use-case is a core design concept behind PIIP.	Yes. This is the primary use-case for the 'alert' functionality in the COSMIC framework.	Yes. This is the use-case envisaged for S189 ECCTA 'warning' scenarios.	Yes, subject to paragraph 4(f) threshold conditions 4(c) requirements to not impact the customer based on information derived from a partnership without further assessing that information.	Yes. This form of collaboration to develop shared adverse information is expected to be permitted.
F.	A tracing function to identify exposure to money laundering/muling dispersals (i.e. a rapid or automated warning chain of alerts to follow transactions across multiple obliged entities, illuminating the network of accounts involved in a dispersal).	Assessed to be possible under 314(b).	Assessed to be possible, but it remains to be developed in practice in an Article 115 Bis platform.	Automated chains of alerts are not envisaged within the COSMIC framework, rather, alerts are single submissions which must be assessed individually by other participants. However, Singapore has an anti-scam legal and operational framework to support tracing and alerts.	Automated chains of alerts are not supported by the ECCTA framework, but such capabilities have been developed in the UK for fraud muling networks through a GDPR legal basis[55]	Automated chains of alerts are not supported by the Article 75 framework.	Yes. This form of collaboration to deliver rapid or automated warning chains of alerts is expected to be permitted.
G.	Combined transaction monitoring	This is not a traditional use of 314(b), however some legal theorists in FFIS events have stated that they believe it is permissible under 314(b).	Yes. This capability is provided for within the 62nd Quarter AML Rule.	This is not envisaged or permitted within the COSMIC framework.	This is not envisaged within the ECCTA framework.	It is arguable that such a capability is permissible under the Article 75 framework, however it would have to be designed in a way that meets paragraph 4(f) conditions and demonstrate strict necessity.	Yes. This form of collaboration through shared transaction monitoring is expected to be permitted.

Legend:

- ✓ This use-case is assessed to be permitted within the P2P AML information sharing law.
- ✗ This use-case is not permissible within the P2P law.
- — It is unclear or contested whether this use-case is permissible within the P2P information sharing law, or there is an alternative law which permits this use-case.

1.5. Private-to-private information sharing related to fraud attack and scam transaction (FAST) money laundering

The money laundering or 'muling' following fraud attacks and scam transactions, which we refer to hereafter as 'FAST' money laundering, has unique characteristics that are relevant to P2P information sharing opportunities.

FAST money laundering characteristics include:

- There is a typically a victim, who can report a crime;
- The moment of the criminal act, and further payment chains, can be visible in financial and payments data held by the private sector (unlike most 'illicit trade' flows);
- Confirmation that a FAST criminal event has taken place can be achieved relatively quickly and can be determined, to a reasonable degree, by a private sector entity without the need for a law enforcement investigation;
- National privacy statutes often provide a legal gateway for P2P FAST threat information sharing and there are potentially other legislative gateways for FAST threat information sharing, such as through payment services regulations (see Table 5 below);
- With the right technical and policy infrastructure, the opportunity to trace FAST money laundering and recover stolen funds is practical and has been demonstrated in a number of countries; and
- There are often stronger commercial incentives for private sector entities to work together to address FAST threats to avoid monetary loss.

These characteristics strengthen the opportunity for information sharing under AML P2P information sharing laws.

In a large number of countries, every FAST event where the proceeds are then passed through the financial system (or through any other obliged entity) can be considered – by definition – an act of money laundering. However, in some countries, money laundering offences exclude FAST as a predicate crime. In these countries, cooperation in relation to FAST money laundering is governed under different a different legal framework compared to AML P2P information sharing.

Where FAST events are considered as predicates to money laundering, and there is an AML P2P information sharing law in place, obliged entities may use the respective AML P2P information law to support information sharing on FAST threats.

It is also important to note, that obliged entities (and other private sector entities) may also use other legislative gateways for FAST risk information sharing. As such, in relation to FAST threats in particular, private sector entities may have a variety of legal options at their disposal for P2P information sharing purposes.

As an example, in the EU, obliged entities have a range of potential enabling legislation for sharing information to detect and prevent fraud and scams and trace the stolen funds.

Table 5. EU private-to-private sector information sharing legal gateways when considering fraud and scam proceeds in the financial system

Policy umbrella	Legal gateway for information sharing
Within the AML/CFT policy umbrella	AMLR Article 75 partnerships can support P2P information sharing on money laundering from an 'all crimes approach', including originating from fraud attacks or scam transactions.
Within the privacy statute	GDPR itself is an enabling framework for sharing information related to fraud attacks and scam transaction risk. As described in the FFIS 'Survey and Policy Discussion Paper: Lessons in private-private financial information sharing to detect and disrupt crime' (2022), several P2P fraud risk information sharing platforms make use of the Article 6(1)(f) GDPR "legitimate interest" basis for sharing information and Recital 47 of GDPR which sets out clearly that "the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."[56]
Within the payment system policy umbrella	While not concluded at the time of this research, a draft[57] of the EU's Payment Services Regulation (PSR) 'Article 83', also provides a (compulsory) legal gateway for information sharing for payment service providers, as follows: • PSR, Art. 83 1.(c): "Payment service providers (hereafter PSPs) shall have transaction monitoring mechanisms in place that (…) prevent, detect and, where possible, resolve potentially fraudulent payment transactions, including transactions involving payment initiation services." • PSR, Art. 83 3.: "To comply with paragraph 1, point (c), payment service providers shall exchange information, including the unique identifier, name, personal identification number, organisation number, modus operandi and other transaction information of a payee with other payment service providers" These provisions are still under legislative consideration at the time of this research. However, the interaction between PSR (possibly mandated) information sharing under PSR and FAST information sharing under AMLR Article 75 will need to be carefully considered.

In countries without an explicit AML P2P information sharing law, there may be other legislation which enables P2P information sharing models specifically for FAST money laundering.

Table 6. Is fraud covered by the respective AML P2P information sharing law (as a predicate crime for money laundering)?

ECR Coverage	USA 314(b)	Mexico Article 115 Bis	Singapore (COSMIC)	UK ECCTA S188 and S189	EU AMLR Article 75	Canada 11.01 Exception
Does the P2P AML law enable information sharing on FAST threats?	✓ FAST money laundering is in scope of 314(b)	– Not permitted under the Article 115 Bis legal framework, but FAST information sharing is possible through other legal means in the jurisdiction.[58]	– Not an explicit feature of the COSMIC enabling framework, but FAST information sharing is possible through other legal means in the jurisdiction.	✓ FAST money laundering is in scope of ECCTA	✓ FAST money laundering is in scope of Article 75	✓ FAST money laundering is in scope of the 11.01 Exception

This study is not intended to be an exhaustive review of the interaction between countries' P2P information sharing gateways across the AML/CFT policy umbrella, the privacy statute and the payment systems policy umbrella. However, in 2025, we observe some level of fragmentation and disconnection between the policy-making process and data sharing legislation being developed across AML/CFT, fraud prevention and payment systems reform – all covering ostensibly the same activity.

Overall, we recommend that each country should achieve a level of policy clarity on how fraud and scams related information sharing and money laundering detection systems connect to each other and are considered holistically by policy-makers.

1.6. The transformative potential of privacy enhancing technologies

The assessment table in Section 1.4 of this study is focused on the sharing of 'raw' underlying data to allow for collaborative analysis on that data. The legal frameworks themselves are generally conceived to provide a legal gateway for information sharing of actual customer data, providing the clear legal framework for that information sharing and ensuring that such information sharing has a potential pathway which is not in breach of data protection laws and does not expose the participating obliged entities to potential civil legal action from the data subject.

However, the field of Privacy Enhancing Technologies (PETs) – which is described in detail in the FFIS 2021 paper, *'Case studies of the use of privacy preserving analysis to tackle financial crime'*[59] – is potentially disruptive to the underlying thinking about what constitutes 'sharing' and what is required to achieve collaborative outputs.

The use of various PETs allows stakeholders to collaborate and receive computational outputs without any requirement to disclose the contributing input data. Such collaboration could potentially allow for some level of the utility from the use-cases described above, without needing to share any sensitive input data.

The integration of PETs within AML/CFT frameworks or specific national ECR collaboration is at a very early stage of development. Explicit guidance about how such PET capabilities interact with data privacy law (from data protection authorities) and how the processes interact with AML obligations for record-keeping (from AML supervisors) are yet to become established in a meaningful way by relevant supervisors.

The EU AMLR Article 75 is the only legal framework that makes reference to the role of pseudonymisation techniques to support the security and privacy of the Article 75 exchanges. How this will be interpreted in practice remains to be seen.

PETs may also help obliged entities to collaborate prior to the point at which an AML P2P law is utilised to provide a lawful basis for sharing personal data or personal identifiable information. That is, PETs can help define potential risk from large volumes of unalerted data which then could be shared 'in the clear' through the relevant legal ECR P2P framework.

In a 2024 white paper, FNA describe the use of PETs to support cross-bank, cross-platform and cross-industry utilities to counter fraud as a means to achieve 'tracing' capabilities without requiring centralised payments data in what FNA term "node-to-node (N2N) architecture".[60] Through one-way hashing of data, financial institutions can be alerted to their exposure to money mule chains, without having to receive any additional data that they did not already possess.

Through such ECR collaboration, data sharing can be minimised and collaboration systems can be designed in a way that no party is provided access to any new personal data and the 'collaborations' only occur when certain objective threshold conditions are met. In the White Paper, FNA describe how node-to-node architectures can apply to post-settlement and pre-settlement risk collaboration and apply to cross-border use-cases.

1.7. Enabling partnership growth: the role for the public sector

Legislation is not enough to support effective ECR P2P collaboration.

A lawful gateway for information sharing provides an ***opportunity*** for information sharing, but – to encourage effective use of the legal gateway – a number of enabling conditions can be put in place.

Echoing the FATF *'Partnering in the Fight Against Financial Crime'* guidelines, we recommend that national policy-makers and supervisors take a number of steps to strengthen the enabling conditions for effective ECR collaboration, even if the expectation is for the private sector to lead in such collaborations.

A. Establish a public-private strategy for leveraging data to respond to economic crime threats.

Information sharing is only a tool to achieve an objective, it is not an objective in itself.

Countries can establish a clear national economic crime data strategy that encompasses the full range of ECR threats - including fraud, anti-money laundering and sanctions evasion - and actively reflects on how their respective partnership framework should contribute to national strategic goals of defence against such threats. This process should involve:

- Policy clarity that the use of information sharing partnerships is required to meet a public interest of tackling economic crime threats and setting out high-level objectives for such information sharing;
- A clear understanding about the data analysis and collaboration mechanisms, across public sector and private sectors, that are required to achieve the overall objectives;
- A clear understanding about the existing data-sharing opportunities and the barriers to data sharing that are relevant to those requirements;
- Ongoing coordination between PPP and private sector partnership designers; and
- Constructive engagement from data protection authorities to help ensure that potential policy conflicts are resolved at the policy-level, rather than contested in the commercial space.

Such a data strategy development process should have public sector and private sector engagement and have levels of governance (and endorsement) at the political, policy, regulatory and operational layers.

B. Encourage alignment between the various supervisors relevant to the information sharing partnership.

Given the fragmentation of regulatory regimes across payments, AML/CTF, sanctions evasion and fraud domains, there will need to be coordination between the respective supervisors. More broadly, ongoing regulatory coordination and engagement will be required to ensure that relevant risks are being managed on an ongoing basis from the perspective of payment efficiency, consumer protection, data protection, competition law and economic crime security considerations.

C. Consider how to strengthen the incentives for ECR collaboration.

Legislation has advanced to support ECR collaboration, but - in general - AML supervisors do not yet recognise the contribution to partnership activity as relevant to the AML supervisory and inspection process. As a result, there is an unclear incentive structure for obliged entities to invest in partnership activity.

The role of governance and supervision will be crucial to ensure that there is a strong incentive (or, potentially, a supervisory expectation) that participant institutions ***contribute*** to risk awareness in a partnership by reporting relevant risks and acting on alerts received.

Currently, this is a major gap in the overall approach to ECR P2P collaboration.

D. Achieve policy clarity on the issue of financial exclusion in relation to preventative measures against economic crime risk.

Finally, and perhaps most importantly, the issue of financial exclusion needs to be managed. Most of the new legislative frameworks set out in this paper place clear legal conditions around the process of making a client exit in response to partnership information sharing. However, there is a still a need to complement the legislative intent with a clear governance framework that allows parties adversely affected by determinations of economic crime risk to challenge the validity of those assessments.

Without compromising the integrity of intelligence related to money laundering, there will need to be robust and transparent mechanisms to ensure that there is a pathway for data correction and redress should innocent parties be wrongly labelled as suspicious in a collaborative economic crime risk assessment system.[61]

Box A: Clarity over the intended treatment of the data subject.
The following discussion box is replicated from the FFIS 2022 report, which goes into much greater detail about a wider range of governance issues associated to ECR platforms.

A policy concern arises if individuals (citizens) are unable to access financial services as a result of a determination of risk which may have been informed by information sharing through a private-private sharing platform.

The emphasis of the AML regime is to prevent access to the financial system of 'illicit funds'. From a FATF perspective, under 'Intermediate Outcome 2' of the design of the FATF approach to effectiveness within the international standards, the AML/CFT regulatory system should ensure that private sector resources are used to help prevent the proceeds of crime and funds in support of terrorism from entering the financial and other sectors or are detected and reported by these sectors.

Financial exclusion is deeply embedded in AML practices in terms of obliged entities making client exit decisions. However, improvements in the ability to achieve FATF Intermediate Outcome 2 through private-private sharing shine a light on the lack of policy clarity about whether it is appropriate or desirable to exclude individuals from the financial system based on suspicion.

In a January 2022 published Opinion, the European Banking Authority raised concern about the scale and impact of de-risking (or exit decisions) in the EU and highlighted that providing access to at least basic financial products and services is a prerequisite for the participation in modern economic and social life. The EBA sets out the need for regulatory and policy level changes to stem "unwarranted de-risking". [62]

The prospect of more consistency between regulated entities in who is denied services brings a policy conflict into sharper focus as to: (1) whether there is a right to financial services and (2) whether it is appropriate to exclude individuals from financial services based on suspicion, set against the traditional predominant outcome of the AML system – i.e. account closures.

Ultimately, this policy conflict is unresolved at the international standards level and private-private information sharing platforms are not in a position to resolve it for policy-makers. Policy-makers will need to determine whether or not financial exclusion, and on what basis, is appropriate and desirable and under what circumstances or threshold of financial crime risk suspicion.

ECR platforms have a greater opportunity to:

- Ensure that accounts are not closed when there is a law enforcement investigative interest to 'keep open' the account.
- Ensure that individuals who have been rehabilitated to society (either as a result of a custodial sentence completed, or as a result of de-radicalisation programme for example in relation to terrorist finance risks) can be provided with a pathway to financial rehabilitation as well.
- To support greater consistency in the effect of certain criminal behaviour and how it might affect an individual's access to financial services – and how long such restrictions may last.

In essence, the growing capability of ECR platforms to produce a more consistent impact against subjects of economic crime risk should encourage policy-makers to be much clearer about what the intended effect against individuals should be.

Chapter 2.

Economic crime risk collaboration at the cross-border level

2.1. The current landscape for international ECR P2P cooperative frameworks

While the policy consensus to enable the private sector to collaborate in response to economic crime threats is increasingly established at the domestic level in advanced economies and major financial centres (as described in the previous Chapter), policy discussions about cross-border ECR collaboration are less well developed – particularly in the fraud domain.

In terms of inter-governmental cooperative 'frameworks' for cross-border collaboration issues – i.e. the extent of international agreements or forums where policy standards and protocols for collaboration are set – the maturity of the policy framework varies considerably between the different domains of economic crime, with cyber-crime arguably the most developed.

In the table below, we highlight information sharing frameworks – and how they differ – between the respective domains of economic crime.

Table 7. Summary of cross-border information sharing relevant to respective ECR threat domains

Domain of economic crime	Current characteristics of cross-border information sharing relevant to that economic crime domain
AML/CTF/CPF	The FATF is responsible for setting the baseline of international standards for AML/CTF/CPF legislation, supervision and arrangements for cross-border information sharing, enforced through a process of country 'mutual evaluations' and with also the threat of 'grey-listing' and 'black-listing' non-compliant countries (including those who are not members of the FATF). Within the FATF standards, cross-border information sharing in the AML/CTF/CPF regime (relating to reported suspicious activity by the private sector), largely takes place through FIU-to-FIU information sharing; i.e. it is envisaged as taking place through public-to-public information sharing. The Egmont group of FIUs, a membership body of FIUs around the world, provides a complementary role within the FATF framework to support more detailed guidance papers and best-practice in FIU-to-FIU cooperation. Beyond suspicious activity and moving into the setting of criminal law investigations, law enforcement agencies around the world can cooperate directly or with the support of policing cooperative forums, such as Interpol or Europol. However, in general, standards and protocols in law enforcement cross-border investigative cooperation are more ad hoc and not explicitly defined by the FATF, as they are for the sharing of financial intelligence through the FIU network. In terms of private-to-private information sharing, the cross-border dimension of information sharing within the FATF standards is historically based on: • Correspondent banking requests for information to determine risk;

	• Payment transparency requirements to enable 'screening'; and • Intra-group sharing within a private sector international enterprise. The FATF framework has not, as yet, required or explicitly enabled obliged entities to cooperate with one another across borders to communicate AML/CFT/CPF risk information or to detect such risk through collaborative analysis.[63]
Sanctions	In the sanctions domain, the details of any sanctioned entities are typically announced publicly by relevant competent public authorities, to varying degrees of specificity, when the entity (or, increasingly, a sector or use-case) is sanctioned. Some aspects of standards to support transparency of information on sending and receiving parties for a payment to travel cross-border (to enable sanctions compliance) are set out at the FATF level through FATF Recommendation 16 (payment transparency obligations). However, in terms of the objective of Recommendation 16, the FATF only refer to compliance with the United Nations Security Council resolutions for sanctions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing. Sanctions issued at the domestic level – for example, by authorities in the U.S., the UK or the EU – are much broader in application and are developed distinctly and outside of a cross-border cooperative framework for defining standards and protocols in this domain. However, largely, they rely on Recommendation 16 in order to be effective. At the private sector level, various third-party vendors are involved in cross-border sharing of risk information related to further understanding money laundering networks used to support sanctions evasion, relying mostly on 'open source' information.
Fraud attacks and scam transactions (FAST)	FAST risk has not benefitted from an inter-governmental standard setter or a dedicated forum for international cooperation to develop agreements and protocols for cross-border information sharing. Fraud risk is shared across borders in certain circumstances, but – as described by financial institutions in FFIS events – it tends to be ad hoc and stakeholders' understanding of what is legally permissible varies significantly.[64] Fraud risk information sharing is typically supported at a domestic level by national privacy statutes, however, the lack of a clear inter-governmental cooperative legal framework and standards regime (akin to the FATF) for fraud risk limits the engagement in developing the legal basis for cross-border information sharing of this risk. In the absence of a standard setting process through the FATF, jurisdictions have sometimes developed their domestic standards for fraud-risk information sharing through the evolution of their 'payment market infrastructure' and associated policy and regulatory regime. However, this is not yet coordinated or standardised at the international level and there are no obvious inter-governmental forums for doing so.

Tax evasion	Tax information sharing has benefited from focused support from the OECD and the establishment of the Common Reporting System (CRS) framework (outside of the U.S.) for sharing information public-to-public.[65] There does not tend to be the same engagement from the private sector to support risk information sharing on tax evasion private-to-private as there is in other domains. However, the J5 Heads of Global Tax Enforcement have established a public private partnership structure to progress tax risk information sharing at the cross-border level (in complement to public-to-public cross-border information sharing between the J5 agencies). This is described in more detail below.
Cyber threats	In September 2024, the UN adopted a treaty Convention Against Cyber-crime,[66] which follows the previous non-UN international legal framework for cybercrime cooperation established by the Budapest Convention on Cybercrime.[67] These treaties establish an international standard for signatory State Parties to develop their domestic legislation on cybercrime and create a clear legal framework for international cooperation between State Parties. While the 2024 treaty is primarily concerned with cooperation between States parties on evidence and criminal law investigations, there are a number of sections which leave open to opportunity to strengthen public-private or private-to-private financial information sharing; not just for traditional cyber threats, but encompassing other ECR threats. These potential opportunities are described in more detail below.

With the passing of the 2024 Convention, and the Budapest Convention prior to that, cyber-security P2P threat sharing is in a strong position out of the economic crime domains in terms of having a dedicated international framework for cross-border information sharing (established under an inter-governmental treaty) and, also, having vibrant eco-system for sharing threat information across borders. The cyber threat domain benefits, to some extent, from much of the information that is shared not being considered protected personal data or personal identifying information.

For the other threat domains – AML/CTF/CPF, fraud, tax evasion and sanctions evasion domains of ECR – there are severe limits on the extent of P2P cross-border collaboration that can currently take place. There is, therefore, a prima facie case to consider how P2P cross-border information can be enabled to help support more effective results in tackling those crimes. The same logic and benefit of P2P collaboration that has driven legislation to enable that activity at the domestic level can potentially extend to the cross-border level as well.

Fraud/scams and associated money laundering is, perhaps, the strongest candidate domain to focus on in terms of developing a cross-border information sharing framework because:

(1) the level of confidence that the information relates to a crime having taken place is often very strong in cases where there is a reported fraud case or an authorised push payment declared (in contrast to other forms of money laundering, which are typically based on identifying suspicion); and

(2) to date, there has been a distinct lack of an inter-governmental forum or standards setting process for how fraud risk information is collected and shared to respond to cross-border threats.

It should be recognised that some countries have tried to initiate cross-border inter-governmental dialogue on FAST money laundering, including:

- In 2023, Singapore hosted a 'Regional Anti-Scam Conference', attended by representatives from 15 countries at which Sun Xueling, Minister of State for the Ministry of Home Affairs and Ministry of Social and Family Development, emphasised the cross-border dimension of the threat and the ease with which FAST money laundering can travel cross-border. The Summit conclusions referenced the need to strengthen cross-border information sharing and establish international norms and standards in this regard.[68]

- In 2024, the UK hosted a 'Global Anti-Fraud Summit', attended by G7 countries, as well as South Korea, New Zealand and Singapore which also issued a communique calling for further international co-operation and collaboration to tackle fraud and scams.[69]

In 2023, the Bank for International Settlements 'Project Aurora'[70] established quantitative measures for the benefit of conducting economic crime analysis at the cross-border level of payments infrastructure and explored the the utility/privacy trade-off considerations of use of privacy enhancing technology to support information sharing cross-border. The report legal and regulatory issues were principal barriers to achieving the benefits of cross-border information sharing related to economic crime risk.

Considering inter-governmental governance across different ECR domains

The projects and multi-national conferences described above have affirmed the absence of, and the need for, a strengthened international cooperative framework for cross-border ECR information sharing, particularly for FAST money laundering.

If cross-border P2P frameworks for AML/CTF/CPF are to be strengthened, then this is highly likely to need to occur through the FATF (as the existing standards setting authority for AML/CTF/CPF).

Protocols and standards for fraud-risk information sharing cross-border *could* be advanced by the FATF or, failing that, through other mechanisms. FATF does not yet have a political mandate to support fraud related standards within the FATF process, however this is theoretically open to change in the future. Outside of the FATF, there are other inter-governmental processes that could fill the gap of the standard setting process for fraud-risk information sharing and the protocols surrounding the transmission and use of that information.

In the next section we highlight a number of innovation track options for strengthening the frameworks, protocols and leadership case study examples to develop ECR P2P information sharing, with a particular focus on fraud risk and the money laundering associated to such theft.

2.2. Options to strengthen cross-border frameworks for P2P ECR collaboration

The primary challenge in cross-border information sharing of ECR risk is the lack of a clear lawful basis for P2P ECR collaboration cross border.

Currently, P2P ECR information sharing across borders is stymied by the lack of a clear positive enabling framework for such information sharing and, in parallel, the restrictive effect of data localisation laws on cross-border transfers of information.

Below we set out 10 potential innovation tracks through which cross-border P2P information sharing, particularly related to fraud, could be advanced. The innovation track options for enhancing the cross-border legal, policy and operational frameworks and protocols for ECR collaboration draw inspiration from advances at the national-level or the EU-level in terms of enabling domestic P2P collaboration to tackle ECR threats.

The first five innovation track options aim to strengthen the international legal framework to achieve a basis for cross-border information sharing and the development of consistent standards and protocols to govern that sharing.

The next five innovation track options refer to options to advance cross-border ECR P2P information sharing that don't rely on inter-governmental agreement on a set of standards for such sharing. Instead, these innovation tracks relate to options that can potentially be pursued, to some extent, in the absence of a more comprehensive inter-governmental protocol through industry and public sector innovation regarding untested or under-developed avenues for exchange of information.

Table 8:

10 FFIS innovation track options for cross-border ECR P2P collaboration

Options to develop inter-governmental standards and protocols to establish, or clarify, the legal basis for P2P ECR cross-border information sharing.	
1.	Support FATF leadership in recognising the importance of private-to-private ECR collaboration at the cross-border level. ***[ECR domain relevance: AML/CFT/CPF, Sanctions and Fraud]***
2.	Update the conception of 'payment transparency' within FATF to cover risk information and tracing capabilities. ***[ECR domain relevance: AML/CFT/CPF, Sanctions and Fraud]***
3.	Utilise the G20's cross-border payment reform process as an engine for cross-border economic crime collaboration. ***[ECR domain relevance: AML/CFT/CPF, Sanctions and Fraud]***
4.	Develop an inter-governmental treaty-basis for international cross-border fraud information sharing. ***[ECR domain relevance: Fraud]***
5.	Establish, or clarify, fraud-risk cross-border information sharing legal gateways on a bi-lateral basis between countries or jurisdictions. ***[ECR domain relevance: Fraud]***
Innovation within existing legal frameworks to develop practice and protocols	
6.	Utilise cross-border sharing opportunities which are permitted in the current ECR P2P legislation. ***[ECR domain relevance: AML/CFT/CPF, Sanctions and Fraud]***
7.	Maximise use of public-public and intra-group (private sector) enterprise-wide sharing across borders as information pipelines to connect insights through various national public-private partnerships and P2P economic crime detection platforms. ***[ECR domain relevance: AML/CFT/CPF, Sanctions and Fraud]***
8.	Expand on existing cross-border public-private partnership intelligence sharing initiatives. ***[ECR domain relevance: AML/CFT/CPF, Sanctions and Fraud]***
9.	Encourage third-party ECR platforms to share their insights cross-border. ***[ECR domain relevance: Fraud]***
10.	Deploy privacy enhancing technologies in cross-border ECR use-cases to share insight on risk, without sharing personal data. ***[ECR domain relevance: AML/CFT/CPF, Sanctions and Fraud]***

These options are unpacked in more detail below. The options are not intended to be an exhaustive set of options, but aim to provide inspiration for industry leaders, policy-makers, supervisors, law enforcement and other innovators in their efforts to drive forward the principles of P2P collaboration at the cross-border level.

Innovation Track Options 1 to 5:

Options to develop inter-governmental standards and protocols to establish, or clarify, the legal basis for P2P ECR cross-border information sharing

i. Support FATF leadership in recognising the importance of private-to-private ECR collaboration at the cross-border level.

Innovation track logic

The FATF is the global standard setter for AML/CTF/CPF issues. If AML/CTF/CPF cross-border P2P collaboration is to be enabled on a consistent international basis, then FATF will be the natural locus for such policy-coordination and for the development of the relevant standards and guidance. FATF currently does not have a standard or interpretative note relating to P2P AML/CTF/CPF information sharing. However, given the rise of P2P AML legislation in a large number of FATF countries (described in this paper), FATF may undertake work to consider such standards and protocols. With a clear political mandate and the required resources, FATF is well placed to develop the standards framework for ***cross-border*** P2P ECR sharing alongside work to draw good practice from its members on domestic P2P information sharing.

Context

The FATF *"Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing"* paper (July 2022) put forward non-binding advisory recommendations for countries to explore the benefits of enabling AML/CTF/CPF P2P collaboration. However, currently, there is no requirement in the FATF Standards for national authorities to establish a legal gateway for private-to-private AML information sharing.

The major economies and financial centres surveyed in this paper have established P2P ECR capabilities at the domestic level in order to enhance overall effectiveness and, in so doing, moved beyond FATF standards to create a new de-facto standard in this regard.

This lack of alignment of the FATF core standards with the practice of major economies and financial centres (as well as FATF's own best-practice papers, described in the introduction) will likely come under some scrutiny over the years to come.

As such, the FATF may take steps to update the FATF Recommendations to take account of advances in AML collaboration and incorporate P2P AML/CTF/CPF collaboration as a more central part of the FATF standards.

As the international standards catch up with national best-practice, there is an opportunity for FATF to take a fresh look at cross-border information sharing, alongside domestic ECR P2P collaboration.

Summary of this option

As the global standards-setter for AML/CTF/CPF, the FATF can establish a project to develop a protocol for cross-border P2P ECR information sharing; drawing from the national experiences in P2P ECR information sharing outlined in this study.

Innovation opportunities

Either at the FATF Plenary level or in the inter-Ministerial meeting that set the political mandate for FATF on a biennial basis[71], a policy and political mandate can be established for FATF to develop a comprehensive project on cross-border ECR P2P collaboration.

Such a project could include:

i. Reviewing the existing national experiences in developing ***domestic AML/CTF/CPF P2P collaboration*** and considering the role for FATF standards to catch up with this leading practice in domestic P2P collaboration; originally outlined in the *"Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing"* best practices paper and now developed in practice across the USA, Mexico, Singapore, the UK, the EU and Canada.

ii. Building on the FATF 'Illicit Financial Flows from Cyber-Enabled Fraud' paper[72], FATF could review the way in which member jurisdictions have ***integrated fraud and ML P2P collaboration*** and consider the role for FATF to support guidance and best-practice papers related to that integration of the threat detection frameworks across fraud and ML.

iii. Moving beyond points (1) and (2) and reviewing domestic P2P best practice, FATF can take forward the required work to develop a protocol on ***cross-border ECR P2P collaboration*** adopt, filling the gap in international standard setting in the fraud P2P collaboration space and the AML/CTF/CPF P2P collaboration issues operate at the cross-border level.

ii. Update the conception of 'payment transparency' within FATF to cover risk information and tracing capabilities.

Innovation track logic

Distinct from the previous Innovation Track (i.e. integrating domestic and cross-border legal gateways for ECR P2P sharing as a requirement within the FATF standards), FATF innovation could relate to updating the conception of 'payment transparency' within the FATF standards to cover risk information and tracing, not just information on sender and receivers of payments for screening purposes.

Context

In the aftermath of 9/11, the FATF established a standard for 'payment transparency' (or what became 'Recommendation 16' of the FATF). The concept was to ensure that accurate sender and beneficiary information travelled with payments, throughout a payment chain. The information was originally intended to allow for tracing of funds, to support financial intelligence objectives and to allow for screening against sanctioned entities.

At the time of this study, the FATF is currently reviewing 'payment transparency' and considering specific revisions to FATF Recommendation 16.[73] With the growth of mobile wallets, payment aggregators, virtual currencies and buy now/pay later services, business models have developed to transfer value between accounts without relying on traditional chain of correspondent banks envisaged in Recommendation 16. The driving policy focus of these revisions is to ensure that originator and beneficiary information can still travel with payments, including in scenarios arising from the development of new payment techniques and service providers beyond banks.

However, these 'payment transparency' proposals do not yet include the opportunity for ***risk*** information to travel cross-border.

The original core objective of Recommendation 16 was that "countries should have the ability to trace all wire transfers"[74] However, this objective has been de-prioritised over the years in favour of screening against names and identifying information.[75]

Summary of this option

The FATF Recommendation 16 is a principal element of the FATF framework for cross-border information sharing. If FATF were to enable the proactive sharing of ***risk*** information through Recommendation 16 (not just identifying information for all payments), it would (1) help deliver the original objectives of Recommendation 16 on tracing capabilities, and (2), more broadly, provide the vehicle the develop the necessary standards and protocols for such cross-border ECR information sharing. In so doing, FATF have an opportunity to leverage Recommendation 16 to allow for the benefits of ECR P2P information sharing, that have been developed at the domestic level, to extend to the cross-border level.

Innovation opportunities

There is an opportunity to evolve the conception of 'payment transparency' within the FATF framework to link payment system integrity with an ability to share risk information through payment processes. A broader conception of payment transparency can facilitate, for example, tracing and understanding payment risk as it is dispersed through money laundering networks or alerting counterparties after a risk has been identified.

Ultimately, FATF Recommendation 16 could then provide for a framework for protocols to develop to that can achieve cross-border risk-sharing capabilities, similar to the national ECR legislative frameworks surveyed in this paper.

Innovation examples

Leveraging payment messaging frameworks and payment infrastructure for detection of financial crime risk is being increasingly developed at the domestic level. In 2023, the Bank for International Settlements 'Project Aurora' concluded that, compared to what could be discovered by individual financial institutions conducting analysis on their own data in silos in rule-based scenarios, analysis at the level of payments infrastructure could be expected to identify 2x to 3x more embedded money laundering networks.[76]

A leading example of a domestic capability to identify money laundering through a payment system operator identified in a FFIS 2022 survey was the Mastercard Vocalink 'Trace' platform, which runs on the UK Faster Payments and UK Bacs payment rails and does not require additional pooling of transaction data beyond what is provided for the operation of the payments frameworks.[77] Vocalink financial crime behavioural models are developed from a data-driven approach, using large-scale payments data from multiple financial institutions and providing intelligence beyond an individual financial institution's partial view. [78] Building on this experience, the UK payment authority 'Pay.UK' initiated a UK 'Enhanced Fraud Data' proof-of-concept on 6-months of historic transaction data, utilising enhanced data sharing through the UK PMI, identified that UK banks could have prevented, on average, 20% more fraud compared to what was identified without the additional data.[79]

In Malaysia, where there is not an explicit AML P2P information sharing legal framework, a 'National Fraud Portal' (NFP) was launched by Bank Negara Malaysia (BNM) and Payments Network Malaysia (PayNet) in August 2024 to support a FAST money laundering detection and prevention capability delivered FNA.[80] By utilising the national payments market infrastructure, the NFP can support automated fund tracing and recovery – where financial institutions can be alerted to their exposure to stolen funds as they are laundered across the entire financial system; limiting the scope for further transfers and increasing the prospect of fund recovery. Between April and November 2024, performance data reported by FNA indicates that the rates of fraud risk funds being frozen increased from 0.5% to 30% and the average time to investigate each case has reduced by 70%.[81] The capability demonstrates how a semi-automated process, leveraging the national payment clearing system, can support management and validation of fraud reports, tracing of money laundering dispersals, sharing alerts to affected institutions and facilitating recovery of stolen funds. NFP data is also used to support risk scoring in the pre-payment settlement phase, to help prevent fraud from occurring in the first place.

iii. Utilise the G20's cross-border payment reform process as an engine for cross-border economic crime collaboration.

Innovation track logic

If FATF does not expand its mandate to cover fraud-risk sharing and cross-border P2P collaboration, then the G20 cross-border payment 'Roadmap' may provide an appropriate alternative vehicle for developing standards and protocols for the lawfulness of cross-border information sharing relevant to fraud and financial crime risk.

Context

The G20 has agreed a *'Roadmap for Cross-border Payments'*[82], which is being overseen by the Financial Stability Board (FSB) and the Bank for International Settlements. The focus of that Roadmap is to reduce the cost and improve the speed, transparency and accessibility of cross-border payments (i.e. addressing 'the challenges'). In February 2023, the FSB published the G20 Roadmap for Enhancing Cross-border Payments: Priority actions for achieving the G20 targets.[83] A major theme of 'priority action' related to 'Aligning Data Frameworks' and, in December 2024, the FSB published its *'Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments'*.[84]

The FSB 2024 paper refers to the laws, rules and regulatory requirements for collecting, storing and managing data, as "data frameworks". The FSB refers to both the AML/CFT system and data protection laws as 'data frameworks'. In what sometimes appears as a conflict, the FSB aim to reduce the friction caused by both sets of data frameworks on the speed of payments, and - also - to reduce the impact of the data protection framework on the information sharing that is required to be shared for AML/CFT purposes alongside payment data. Because there is no standard setter for fraud information sharing, there is no 'framework' for the FSB to refer to for fraud risk information sharing.

The FSB has determined to establish a Forum comprised of the diverse set of public sector stakeholders relevant to cross-border payments, including payments, AML/CFT, sanctions, and data privacy and protection stakeholders to develop relevant standards and protocols. The Forum would lead on:[85]

- Promoting the alignment and interoperability of regulatory and data requirements related to cross-border payments. The implementation of rules and standards concerning the data needed to accompany a cross-border payment transaction is not always uniform across jurisdictions. Fragmentation has been observed in the inconsistent implementation of FATF standards, messages and clearing requirements, as well as data requirements related to sanctions regimes. Recommendations in this area also include promoting the interoperability of data protection and privacy regimes and appropriate cross-border transfer mechanisms for payments-related data.

- Mitigating restrictions on the flow of data related to payments across borders. Measures that require data to be stored or processed in-country (data localisation) or require

maintenance of the data in the local jurisdiction (data mirroring) can undermine Roadmap objectives. While such data-related requirements may have legitimate public policy objectives, they may also make it more difficult to identify fraud, comply with AML/CFT and sanctions obligations, and manage risk on an enterprise-wide basis. The recommendations aim to open up trusted avenues for the cross-border flow of data related to payments.

- Reducing barriers to innovation. Technological innovations that may offer solutions to data frictions could help improve the efficiency of the payments system but appear to be difficult to implement. The recommendation aims to encourage progress on promising innovations and developing frameworks that support public and private sector work.

The FSB report does not get into any details about specific data attributes or fields and their relevance to specific objectives in financial crime or fraud prevention. However, in Recommendation 9 of the paper, the FSB call on **"**Recommendation 9: National authorities should provide a clear and reasonable legal pathway for cross-border payments market participants to transmit across borders data related to payment processing, risk management, or fraud and financial crime prevention. Where applicable, national authorities should provide alternatives to requirements to use local computing facilities."[86]

Further, the FSB refer to the need for governments to encourage "technologies that allow for data sharing in protected environments, full payment traceability, improved customer verification and pre-payment validation, among others."[87]

Summary of this option

The G20 cross-border payment reform process, coordinated through the FSB and the BIS, can provide the international framework for developing the protocol for ECR P2P collaboration, leveraging and aligning with the technical and policy work ongoing to enhance cross-border payment systems.

Innovation opportunities

The FSB's 2024 paper is a significant policy intervention, which – in effect – encourages national policy-makers to provide supremacy to the need for information sharing related to payments data and relevant fraud and financial crime risk data over (some) data protection restrictions.

This type of G20-level intervention may provide an overall guide for nations to avoid conflict between data protection considerations and cross-border information sharing requirements to protect payment systems from fraud and other economic crime risks. ECR stakeholders in the private sector, public sector and academia now have an opportunity to explore what the FSB's Recommendation 9 means in practice – in the interests of a safe and secure cross-border payments framework that also delivers on the G20's mission for faster, cheaper, more accessible and more transparent cross-border payments.

As a next step for innovation in this regard, industry leaders may describe what data is useful to share cross-border for specific fraud and financial crime use-cases (and, therefore, what is proportionate in balance with data protection considerations).

iv. Develop an inter-governmental treaty-basis for international cross-border fraud information sharing.

Innovation track logic

If FATF does not expand its mandate to cover fraud-risk sharing and cross-border P2P collaboration, then a new non-FATF framework to clarify the lawfulness of cross-border information sharing may need to be established. An inter-governmental treaty could provide such a basis or an existing treaty for cyber-crime related information sharing could be developed for the purpose.

Context

Standards-setting in the AML/CTF/CPF domains of economic crime are clearly supported by the FATF, which ensures a framework for inter-governmental dialogue and a set of legal standards to achieve consistency and effectiveness, underpinned by guidance 'interpretative notes' and supported by an evaluation process. However, the FATF does not provide a standards framework nor guidance related to how countries tackle fraud and scams. As such, a new treaty basis – or leveraging an existing treaty – may be required to achieve an international cooperative framework for the threat of fraud. Such a treaty-basis can provide the legal framework for international protocols for P2P information sharing to enable the private sector to communicate regarding fraud risk, proactively send risk warnings and/or collaborate to support tracing of money flows across borders. Such capabilities can ultimately enable preventative measures to reduce the scope for cross-border money laundering of fraud and, where it has occurred, to support the tracing of those funds and the recovery of stolen funds, where possible.

In September 2024, the UN adopted a treaty Convention Against Cyber-Crime[88] which follows the previous non-UN international legal framework for cybercrime established by the Budapest Convention on Cybercrime.[89] These frameworks could either provide an example for a new treaty-basis for intergovernmental and public-private cooperation on fraud or, alternatively, could provide *the* framework to support fraud P2P cross-border information (subject to further policy innovation and development), given the dominance of cyber-enabled forms of fraud.

However, this wider interpretation of the Convention Against Cyber-Crime would require industry and government leadership and policy consensus behind it.

Summary of this option

By establishing, or leveraging, an inter-governmental treaty-basis for P2P information sharing to tackle fraud, legal clarity could be achieved to enable the cross-border P2P and PPP collaboration capabilities with respect of fraud. The recent adoption of the UN Convention Against Cyber-crime may provide opportunities to develop the fraud P2P collaboration protocol.

Specific innovation opportunities

There are pathways within the 2024 Convention Against Cyber-crime for developing an inter-governmental protocol related to P2P collaboration to help detect, prevent, trace and recover the proceeds of fraud. The Convention includes provisions under Article 31 for countries to develop "identification, tracing, freezing or seizure of any [proceeds of cyber-crime]"[90], and under Article 53, 'preventative measures', the Convention specifically promotes the participation of the private sector entities in prevention activities, stating that preventative measures can include strengthened cooperation with law enforcement and "preventing and detecting transfers of proceeds of crime and property related to the offences established in accordance with this Convention."[91]

The normal process for further development of what these Articles mean in practice is that they are discussed and best-practice is shared through a 'Conference of States Parties', which under Article 57 will take place "not later than one year following the entry into force of the Convention and, thereafter, […] regular meetings of the Conference shall be held."[92] Article 61, covering 'Relation with protocols', sets out how protocols may be developed to supplement the Convention, subject to achieving the quorate support from states parties.

In an ideal world, a new treaty basis might be established for governments to cooperate and to provide a legal basis for information sharing between the private sector to tackle fraud. However, in the absence of such a treaty and the long timelines involved in developing such Conventions, it is arguably more practical to focus on leveraging the existing available Conventions for the same purpose.

While not explicitly referencing fraud in the title, the Convention Against Cyber-crime includes cyber-enabled fraud crimes within scope and can provide a framework for governments to work together to develop and clarify a set of protocols for P2P information sharing.

A cross-border P2P protocol for fraud-risk financial-sector information sharing can be developed and implemented, with the support of governments, industry and academia, and form best practice under the Convention Against Cyber-crime in the implementation of Articles 31 and 53 (that set out the explicit purpose of enhancing detection and prevention of the crimes through cooperation with the private sector and enabling the identification, tracing, freezing or seizure of proceeds of cyber-crime) or a formal update Protocol to the Convention could be put forward by States Parties.

v. Establish, or clarify, fraud-risk cross-border information sharing legal gateways on a bi-lateral basis between countries.

Innovation track logic

If the FATF does not expand its mandate to cover fraud-risk sharing and cross-border P2P collaboration, and there is no available inter-governmental framework to leverage for developing such standards (such as an inter-governmental treaty or the G20 Roadmap for Cross-border Payments), then industry and policy-makers can focus on developing bi-lateral frameworks for clarifying the legality of cross-border fraud-risk information sharing between the respective jurisdictions. Jurisdictions could proceed on this innovation path, in parallel to pursuing the longer process of multi-lateral inter-governmental agreement on legal frameworks.

Context

A common characteristic of the early process for domestic ECR PPPs was that they sought to make use of the existing national legal framework to find opportunities for public-private information sharing that had not been utilised before. ECR PPPs demonstrated the value of operational collaboration through innovative interpretation of existing laws (that had not been necessarily designed specifically for the purpose of establishing an ECR PPP).[93]

It is likely that, through analysis of country pairs, there can be legislative pathways identified that enable forms of cross-border ECR P2P collaboration that, hitherto, have not been commonly utilised for that purpose, or – where it has been used – it is subject to some uncertainty by virtue of no clear endorsement of the legal corridor by respective policy-makers and data protection authorities.

New interpretations of existing laws may give rise to some uncertainty. Therefore, innovation in interpretation related to ECR cross-border collaboration 'corridors' would benefit from being acknowledged and affirmed by public sector authorities through a process that gives confidence to the private sector stakeholders involved.

Through such a process, countries that see cross-border collaboration on fraud risk as a high priority could develop relevant cross-border protocols without waiting for more comprehensive international agreement on such protocols.

Summary of this option

With policy and data protection authority support, bi-lateral 'corridors' for cross-border P2P ECR information sharing capabilities may be able to be established, or, rather, their presence confirmed and endorsed without changes to the existing legal framework. Absent a comprehensive inter-governmental treaty basis for legal clarity in cross-border fraud information sharing, some cross-border ECR information sharing capabilities may be possible through innovative use and fresh interpretation of existing laws in specific jurisdictions.

Specific innovation opportunities

With policy, political and private sector support, a process of deep analysis of existing laws to find the legal pathways for some form of practical innovation can then be applied for ECR P2P collaboration at the cross-border level on a bi-lateral basis.

A network of bi-lateral 'corridors' for ECR collaboration may even be established and strengthened, by multiple countries establishing or affirming the respective bi-lateral information sharing corridors.

Some industry experts, interviewed by FFIS, believed that there were already many legal gateways for bi-lateral fraud risk information sharing between countries and there are, more ad hoc examples of successful bi-lateral cooperation between countries. However, these corridors for information sharing have not necessarily been promoted or publicly acknowledged by governments.

When legal gateways are 'untested' and 'unconfirmed', there is – inevitably – a disincentive for the private sector to make use of such legal gateways. Policy clarification could encourage cross-border fraud private-to-private collaboration in cases where there is an arguable legal basis for such information sharing already in place. This process of legal innovation and affirmation can be a useful function of 'sandboxes' established by data protection, fraud prevention and AML supervisors.

Innovation Track Options 6 to 10:

Innovation within existing legal frameworks to develop practice and protocols

vi. Enhance cross-border use of the current ECR P2P legislation.

Innovation track logic

To a limited degree, the new wave of ECR P2P 'domestic' legislation provides room for some elements of cross-border sharing. These should be explored and utilised.

Context

As described in this paper, P2P ECR collaboration legislative regimes in Mexico and the EU present the strongest opportunity for P2P information sharing to occur cross border and opportunities also exist in the Singapore and U.S. regime for the more limited use-case of enterprise-wide intra-group ECR sharing.

Pursuant to the 62nd Bis, Ter and Octies of the AML/CFT Rules, Mexican banks may exchange information of their customers' operations with similar Foreign Financial Entities, while certain SARs information can be shared cross-border with group, subsidiaries and correspondent banks.

The EU AMLR Article 75 provides for AML/CTF collaboration across borders (intra-EU member states). The first cross-border Article 75 partnership proposal is yet to emerge at the time of this study, but it seems likely that there will be a cross-border Article 75 partnership in operation across borders (within the EU) in a matter of years.

In Singapore, the Monetary Authority of Singapore permits such sharing of information that financial institutions receive from COSMIC to both their local and overseas affiliates, only for group-wide ML/TF/PF risk management purposes, on a need-to-know basis and provided that additional conditions are met. Financial institutions are required to comply with additional safeguards when sharing to individuals outside of Singapore.[94]

In the U.S., while there are no specific enabling features within U.S. 314(b) legislative framework to share information across borders, such sharing is *not prohibited*. In addition, FinCEN have actively promoted and encouraged U.S. financial institutions to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity. [95] FinCEN is also clear that U.S. financial institutions that the sharing of underlying account or transaction information does not violate Suspicious Activity Report (SAR) confidentiality restrictions in the BSA and FinCEN's regulations unless such sharing would potentially reveal the existence of a SAR.[96]

Summary of this option

Out of the six jurisdictions surveyed in this paper that have developed domestic legal frameworks for P2P ECR collaboration, the Mexican legislative framework has specific enabling features for cross-border ECR P2P collaboration and the EU Article 75 permits intra-EU cross-border sharing. The Singapore and U.S. regimes for P2P information sharing also present some, more limited, opportunities for information sharing cross border intra group and possibly beyond. These opportunities can be leveraged and explored.

Innovation opportunities

Cross-border P2P collaboration opportunities arising from the new and existing P2P ECR legislation at the domestic level present various opportunities and challenges. Each has its own complexity with regard to the geographic limit, the ECR threat coverage, the purpose limitation and potential limits to the safe harbour of such sharing.

However, there are still obvious opportunities to leverage cross-border information sharing through these legal gateways.

At the EU level, there may be further opportunities for cross-border AML collaboration between (1) EU-member states and (2) countries with GDPR-aligned or equivalent privacy regimes. Subject to further policy clarification and policy support for such an endeavour, it seems reasonable that cross-border sharing between countries like the UK and jurisdictions like the EU, through a form of Article 75 partnership may be able to progress if it can be demonstrated to add value to the awareness of risk in both jurisdictions.

Innovation examples

In November 2024, FFIS and the Bank for International Settlements Innovation Hub Nordic Centre organised a workshop on the design of a cross-border AMLR Article 75 partnership to include all three Baltic jurisdictions. The event included delegations from all three EU members states, including AML supervisors, FIUs and major financial institutions. Exploratory work on the first cross-border Article 75 partnership proposal is ongoing at the time of this paper.

vii. Maximise use of public-public and intra-group (private sector) enterprise-wide sharing across borders to connect insights through various national public-private partnerships.

Innovation track logic

Not requiring legislative change, there are opportunities to establish information sharing 'pipelines' through either (1) public-public information sharing; and/or (2) through intra-group private sector sharing cross border to enable information flow between existing domestic P2P and PPP collaborations.

Context

Public-public information sharing between law enforcement agencies in different countries can provide a structured way to ensure that cases and risk information, as well as broader typologies or threats, can be shared between different domestic PPPs internationally.

However, in some cases, an ECR partnership will only involve private sector entities. In this case, it may be possible to connect operational insights between partnerships through a single financial institution that is a member of two different national-level P2P collaborations.

Jurisdictions are encouraged by the FATF to allow multi-national private sector obliged entities to be able to share risk-information across their enterprise group, with affiliates, across borders. The FATF has supported legal reforms to limit the impact of data-localisation laws preventing a single financial group from observing, analysing and responding to risk as it exists across their international business lines.[97]

While there are still restrictions in some countries for an international financial institution to share risk information within their group, many countries have enacted reforms to support intra-group sharing across borders.

Where legally permissible and subject to appropriate governance, record-keeping and accountability mechanisms, intra-group sharing may be a useful pathway to allow insights or operational information to pass from one PPP or P2P to a counterpart PPP/P2P in another country. In other cases, public-to-public sharing pipelines could be developed in a more structured way to connect between private sector entities and allow a form of cross-border P2P collaboration.

Summary of this option

Through the appropriate protocols, information sharing 'pipelines' available through public-to-public sharing across borders (through law enforcement authorities, or through Financial Intelligence Units, to their counterparts) and/or private sector (intra-group) sharing can link up domestic PPPs or P2Ps to enable cross-border collaboration.

Specific innovation opportunities

Arising from the growth of public-private partnerships around the world[98] and the expected growth of P2P ECR collaboration partnerships, we can expect the body of collaborative insight on ECR threats to expand at the domestic level.

The pathway for cross-border sharing between PPPs and P2P partnerships through the intra-group sharing of their members is an under-explored and under-clarified gateway for cross-border information sharing. With careful consideration and involvement of leading PPPs/P2Ps, a protocol can be established for how intra-group sharing can and should provide a corridor between through partnerships.

In the absence of a protocol being developed, some jurisdictions have opted for a complete prohibition on intra-group sharing being then passed on to national PPPs or P2Ps. For example, the Singapore COSMIC framework actively encourages intra-group sharing but only for sharing within the same entity. Onward sharing to another PPP or P2P is not permitted.

Likewise in the UK, intra-group sharing has been actively supported through policy reforms,[99] but the use of P2P information sharing under ECCTA powers only provide a legal protection for domestic information sharing and does not extend to intra-group cross-border sharing.

This lack of clarity, to some degree, can be addressed by the PPPs and P2Ps themselves, particularly with the support of further policy development and guidance. Countries may choose to develop protocols for intra-group sharing between PPPs/P2Ps on a bi-lateral basis and such innovation could serve as an example for a broader inter-governmental protocol for inter-PPP/P2P collaboration.

Those jurisdictions with active PPPs and a policy commitment to enable intra-group sharing can lead in developing protocols for such information sharing across borders from insight developed in their respective domestic PPP or P2P partnerships.

It is reasonable to expect that intelligence shared or developed within partnerships should come with classifications about the releasability of that information to other AML partnerships, in the same way that traditional national intelligence is shared across borders between public sector agencies within an intelligence alliance.

Policy examples of intra-group sharing

In the U.S., FinCEN, alongside federal banking agencies, have issued guidance on sharing SARs by U.S. financial institutions with their Head Offices and affiliates. Under the guidance, "[a] U.S. branch or agency of a foreign bank may share a [SAR] with its head office outside the United States for these purposes. Similarly, a U.S. bank…may disclose a [SAR] to its controlling company, no matter where the entity or party is located. In the event that a [bank's] corporate structure includes multiple controlling companies, the filing institution's [SAR] may be shared with each controlling entity."[100]

In the EU, the 4th Anti-Money Laundering Directive (4AMLD), Articles 45(1) & (8) stipulate that "Member States shall require Obliged Entities that are part of a group to implement group-wide policies & procedures, including data protection policies and policies & procedures for sharing

information within the group for AML/CFT purposes" [101]; and "Member States shall ensure that the sharing of information within the group is allowed. Information on suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the group, unless otherwise instructed by the FIU." [102]

In the UK, guidance issued in 2020 published by HM Treasury and the Home Office promotes information sharing within corporate groups. "Information sharing on a group-wide basis is a useful tool to prevent, recognise, investigate, and report specific cases of ML/TF. It also enables global risk assessments, which corporate groups should undertake across all branches and majority-owned subsidiaries as the basis for their whole-group policies."[103]

While these examples illustrate policy support for intra-group information sharing within multi-national obliged entities in the private sector, there are currently no public examples of clear guidance about how an obliged entity can connect insight achieved through their participation in a domestic PPP through their group (and potentially on to a different PPP in another jurisdiction).

viii. Support third-party analytical ECR platforms to share their insights across borders.

Innovation track logic

Third-party analytical ECR platforms already see cross-border risks by virtue of understanding risks associated to the counterparties of their clients. However, the extent to which this information can be shared back to entities in the country where the risk resides is under-explored from a policy and practical perspective.

Context

Third-party technology platforms supporting AML collaboration or other financial crimes risk management services to multiple obliged entities have the potential to see connected risk across borders within their business data.

Often those third-party platforms will also have relevant risk information related to counterparties of their clients (i.e. clients of financial institutions that are not members of that platform) and this could extend to a significant awareness of risks in countries where they have no client financial institutions as members.

Currently, there is ambiguity and a lack of clarity as to what extent these platforms can share this information back with stakeholders in those jurisdictions to alert them to this risk, including to support risk awareness in domestic ECR P2P collaboration platforms in that second country.

As domestic ECR P2P platforms grow, by virtue of the enhancements to the domestic legal environments surveyed in this paper, they will discover more risk – at the level of the platform – relevant to other jurisdictions. There is a case for allowing this risk information to be shared back to counterparty P2P ECR platforms or obliged entities in that jurisdiction.

Summary of this option

Cross-border ECR risk information can be observed by some ECR third-party analytics platforms, existing and operating today, through corresponding visibility of counter-party behaviour across borders. Policy clarity can be achieved about the extent to which ECR platforms themselves can share information across borders and the extent to which they can share their awareness of risk to other jurisdictions where they have observed risk but do not necessarily have operations or clients.

Innovation opportunities

Policy-makers could clarify the opportunity that those third-party analysts have to share the 'birds-eye' view of risk across borders.

Policy-makers should consider how to ensure that this risk information is not siloed by data localisation laws, but integrated into an appropriate information sharing framework, with adequate governance and oversight, which enables the broader awareness of risk that can better detect financial crime threats.

This could first be achieved through bi-lateral or multi-lateral agreements between countries, which could then develop as good-practice for other countries to adopt.

Innovation examples

Under the U.S. 314(b) framework, Nasdaq Verafin provides a cloud-based software platform for financial crime management, including fraud detection, AML compliance, high-risk customer management and information sharing under the 314(b) framework in the US. Nasdaq Verafin can enable investigative insights and machine learning analytics by leveraging its consortium-level data from its client base, including:

- 2,600 financial institutions that use its transaction monitoring, analytics and investigation platform for fraud detection and anti-money laundering;
- Payments data covering over 650 million counterparties; and
- Monitoring of over a billion transactions per week and underlying value of USD 10 trillion in collective assets in members' customer accounts.

This unique data set has enabled Nasdaq Verafin to develop risk intelligence covering counterparties of transactions and payments, including international accounts and entities outside its network. Nasdaq Verafin can leverage analytics from this consortium data to provide risk intelligence and risk scoring to clients in various jurisdictions, without necessarily sharing personal data across borders.

ix. Expand on existing cross-border public-private partnership intelligence sharing initiatives.

Innovation track logic

Cross-border ECR public private partnerships exist and can play a role to enable some of the other innovation track options laid out in this paper.

Context

At the 2022 FFIS 'Conference of Partnerships', a major event for PPP and P2P public sector and private sector decision makers to come together, a number of cross-border partnerships were represented including the Europol Financial Intelligence Public Private Partnership (EFIPPP); The J5 Joint Chiefs of Tax Enforcement and the Global Financial Institutions Partnership (GFIP); and Quad Island Forum of Financial Intelligence Units - Private Public Partnership Forum.

These partnerships typically exchange strategic information about trends and typologies, but – in some cases – do exchange operational information.

There are a much wider range of public-private partnerships in operation in cyber defence domain of economic crime, such as the Cyber Defence Alliance, that have a stronger track record in sharing operational information across borders; though often focused on cyber threat identifiers, rather than traditional personal data.

A gap remains in terms of supporting ECR P2P collaboration at scale through these PPPs and leveraging the cross-border PPPs to achieve advances on other innovation tracks identified in this study.

Summary of this option

There are a number of cross-border public-private partnerships relevant to AML threats already in existence. These partnerships could be leveraged as a vehicle for expanding and supporting P2P cross-border ECR sharing, in complement to their PPP activity already taking place.

Innovation Opportunities

Existing cross-border PPPs should be seen as enablers for advancing the other innovation tracks described in this paper.

Through the engagement of public and private sector members of the respective partnerships, those cross-border partnership can be at the forefront of achieving practical advances in innovation in P2P ECR information sharing.

The respective cross-border PPPs also can support in terms of illuminating the policy, legal and regulatory issues that inhibit the development of ECR P2P cross-border use-cases of priority interest to that PPP.

Finally, cross-border PPPs can position themselves to be engaged customers of information developed through P2P ECR collaboration to help address the threats through additional measures, including law enforcement action where appropriate.

Innovation examples

See below a description of the cross-border partnerships, referenced above and participating in the 'Conference of Partnerships 2022':

The Europol Financial Intelligence Public Private Partnership (EFIPPP)

Established in 2017, the EFIPPP provides a cooperative mechanism between private sector stakeholders, Financial Intelligence Units (FIUs) and investigative authorities to develop and share strategic threat information (e.g. financial crime typologies) between members. The Secretariat of the EFIPPP is located within the European Financial and Economic Crime Centre (EFECC) at Europol.

EFIPPP has established a number of working groups and work streams designed to help improve members' awareness (private sector, FIUs and investigative authorities) of relevant criminal trends and typologies and to identify opportunities to address financial crime threats in a more collaborative and cooperative way. EFIPPP currently has around 100 members institutions and observers from across the EU and some third countries.

The J5 Joint Chiefs of Tax Enforcement and the Global Financial Institutions Partnership (GFIP)

Established in 2018, the Joint Chiefs of Global Tax Enforcement (J5) is a global joint operational group to combat transnational tax crime. Composed of the Australian Taxation Office (ATO), the Canada Revenue Agency (CRA), the Fiscale Inlichtingen- en Opsporingsdienst (FIOD), Her Majesty's Revenue & Customs (HMRC), and Internal Revenue Service, Criminal Investigation (IRS-CI), the J5 members work together to gather information, share intelligence, conduct operations and build the capacity of tax crime enforcement officials. In 2022, the J5 Summit included a launch for the Global Financial Institutions Summit which would later become the GFIP.

GFIP is committed to working towards common goals in tackling tax crime through collaborative efforts, identifying new opportunities to encourage breakthrough thinking and recommendations for future working. Subject matter experts from across public and private sector shared knowledge and expertise, develop opportunities for PPP working, and have committed to resource a programme of work in the year ahead with a view to developing guidance products for wider sharing with law enforcement and private sector partners.

Quad Island Forum of Financial Intelligence Units - Private Public Partnership Forum

The Financial Intelligence Units ("FIUs") from the Crown Dependencies of Guernsey, the Isle of Man and Jersey and the British Overseas Territory of Gibraltar established the Quad Island Forum of Financial Intelligence Units (QIFFIU) to enhance collaboration in respect of sharing intelligence, operational and tactical objectives in the international fight against money laundering, terrorist financing and proliferation financing.

The QIFFIU recognises the importance of public-private exchange and international cooperation in the fight against money laundering, financing of terrorism and proliferation financing.

In 2021 the QIFFIU set-up the Private Public Partnership ('PPP') Forum, the principal objective of which is to gather and share good practice in the development of PPP and to assist in the establishment process for individual PPPs within each of the Quad jurisdictions.

The QIFFIU is cooperating with the UK National Economic Crime Centre to develop a real-time 'cross-border' interaction with the UK Joint Money Laundering Intelligence Taskforce (JMLIT). Historically, there was no mechanism in which the JMLIT can operationally cross-check the JMLIT requests with the private sector regulated entities in the respective quad islands and territories.

x. Deploy privacy enhancing technologies in cross-border ECR use-cases to share insight on risk, without sharing personal data.

Innovation track logic

Cross-border ECR P2P collaboration can be enabled by the use of Privacy Enhancing Technologies (PETs). Such innovative technologies allow for computational results to be shared, without requiring the disclosure of the contributing input 'raw' data, including personal data. By so doing, PETs can support ECR collaborative analytics to be compliant with existing data protection frameworks, while opening up new use-cases for forms of cross-border sharing of insight.

Context

FFIS has previously highlighted national domestic level financial crime detection pilots, use-cases and commercial deployments of privacy enhancing technologies to facilitate the sharing of insights, without the need to share or expose underlying data.[104] Due to the larger data protection and legal barriers for sharing information at the cross-border level, there is likely to be a greater utility for privacy enhancing technology in such cross-border use-cases.

The first theories relating to privacy enhancing technology and privacy preserving analysis, as we now understand it, were developed in the 1970s. The theories found life in mathematical and cryptographic models in the 2000s, but were typically too expensive in computational cost to be practical. In recent years, as a result of advances in the underlying techniques and reduced cost of computational processing power, PETs have started to be deployed in real-life scenarios – with national intelligence and healthcare as key sectors of early adoption. Since 2019, the development of PETs in relation to AML and financial crime prevention have been spurred by significant and supportive activity by several AML supervisors.

PET capabilities raise additional options for policy-makers and industry practitioners and should encourage dialogue about how these advances in technology can be supported by policy frameworks and there can be clarity of the permissibility of the techniques in certain use-cases. When policy-makers and/or industry practitioners are clear about the type of collaboration they wish to permit in cross-border ECR P2P use-cases – and what contributing information they wish to remain undisclosed (not shared across borders) within that process, and by whom – then PET technology can be applied to such use-cases. The UK-US PET Prize of 2023[105] focused on financial crime use-cases and, in 2024, the Bank for International Settlements 'Project Aurora'[106] also highlighted the potential of privacy enhancing technology to support machine learning analysis and other forms of collaboration across borders, mapping the utility benefit and privacy gain across various theoretical use-cases.

Summary of this option

PETs can allow for various forms of shared computational analysis, without sharing underlying input data. PETs can have a transformative effect on ECR collaboration and enable forms of interaction without needing to disclose underlying data, thereby protecting the participating obliged entities from data protection related risks.

Innovation opportunities

PETs could support a number of ECR capabilities for collaboration, described in this paper, without disclosing personal sensitive data.

Under this innovation option, the private sector can potentially make progress without policy and legislative reform. Industry innovators could develop use-cases for cross border sharing and demonstrate the value of PETs to provide for security and data minimisation benefits, and – crucially – compliance with existing data protection laws.

However, as the FATF highlighted in the *'Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing'*[107] best practices paper, the engagement of policy-makers can help support this innovation – particularly from a data protection perspective – to emphasise and publicly promote the advantages achieved through the PET techniques in a technology neutral manner.

The role of industry and policy-makers is to work together to ensure these use-cases comply with data protection and economic crime legislation, with relevant safeguards in place. Industry can push the boundaries of innovation in this area and explore the latest capabilities, but this is more likely to occur with a level of support from public agencies.

Innovation examples

The Swift Industry Pilot Group (IPG) to tackle cross border payments fraud is an example of industry leadership in driving forward innovation to support cross-border ECR collaboration through the use of PETs.[108]

As part of the IPG, Swift has convened 10 leading financial institutions (including BNY, Deutsche Bank, DNB, HSBC, Intesa Sanpaolo and Standard Bank) to test how it can use advanced artificial intelligence (AI) technology to analyse anonymously-shared data from different sources. The pilot will test the use of secure data collaboration and federated learning technologies. Swift's AI anomaly detection model is then intended to gather insights and identify potential fraud patterns from a much richer dataset cross-border.

In this pilot, Swift is using its cross-border view of payments in connection with data at the level of the participation financial institutions, in privacy preserving framework, with a view to test a number of the private-to-private sharing capabilities, including:

- to run a federated learning risk detection model capability;
- to alert members of the IPG to fraud risk that has been identified by a single member; and
- potentially, to move forward with a combined transaction monitoring capability operating between the group in privacy preserving manner.

Federated learning, whereby an AI model is sent to each participating bank to be further trained on localised data in a compute environment controlled by the bank, will help AI models learn from wider data sets compared to what a single financial institution can access.

Swift has three main objectives for the pilot:

1. Demonstrate the business value that can be generated for Swift's customers (and their customers) in better detection and prevention of fraudulent transactions through secure data collaboration and federated learning; first demonstrate with artificial data and then with real data for real-world applications.
2. Assess whether privacy enhancing technologies are sufficiently mature to be deployed in production environments to serve the global financial industry, whilst adhering to the highest standards of security, privacy and risk management.
3. Stimulate the dialogue at a global level for the need for industry-wide, international collaboration to solve the challenges in financial crime detection with all involved parties.

The IPG capabilities are intended to offer risk detection scores at the following stages of a transaction:

- Pre-processing, allowing Financial Institutions to query the anomaly detection capabilities developed by Swift via its payment pre-validation API and before the initiation of a payment;
- In flight, allowing Financial Institutions to alert payments sent on the Swift network if those are detected as abnormal as per the appetite of the Financial Institution; and
- Post-processing, allowing Financial Institutions to review post-fact sent payments against various patterns of anomaly as per the appetite of the Financial Institution.

Swift is developing a "financial crime prevention sandbox" and, in 2025, will run two experiments in the sandbox. These experiments will focus on mule account and fraud label sharing.

The secure data collaboration and federated learning platform envisioned will have the following core principles:

1. Financial institutions govern their own data through the entire lifecycle of the collaboration.
2. End-to-end encryption of customers' data: at rest, in transit and during computation.
3. Verifiable attestation to allow a zero-trust security framework.

Swift has developed an AI Governance framework, aligned with industry standards such as ISO 42001, the NIST Framework for Trustworthy AI and industry Responsible AI Principles[109], to guide all AI development. In addition, Swift is also in the process of implementing a model risk management framework to manage the lifecycle of the AI models being deployed, ensuring auditability, explainability and fairness in the AI analytical process.

Conclusions

This paper charts out the intense period of legislative reform that has taken place to enable ECR P2P collaboration at the domestic level, now covering some of the largest and most advanced economies and financial centres in the world.

However, legislation is not enough for effective P2P ECR collaboration to grow.

A key challenge in 2025 is the one of the incentives for collaboration. Most of the legal gateways created are voluntary and, at present, largely inconsequential for AML supervisors. Even as collaboration demonstrates more effective results, the incentive structure created by supervisors to invest in such collaboration remains weak. Significant changes are now required by supervisors, to adapt to the new era of collaboration, and consider their own role in stimulating private -sector activity and investment in P2P collaboration.

At the cross-border level, there is still much to do. Almost all money laundering, of any organised nature, is cross-border. However, the legislative response explored in this paper is still largely domestic.

Industry pilots, such as the Swift IPG, can provide greater clarity on the opportunity of technology to help improve awareness of risks across borders, but, ultimately, policy-makers are responsible for ensuring that clear cross-border data sharing frameworks are established and are able to respond to the threats that their societies are facing. Furthermore, this pilot programme is likely to enhance understanding about how AI can contribute to AML/FT purposes.

Policy-makers, industry leaders and supervisors should now take inspiration from the initiatives at the domestic level on P2P collaboration and explore how the same benefits could be achieved at a cross-border level. The 10 innovation track opportunities set out in this paper aim to provide a basis for that further exploration by those stakeholders.

We see a key opportunity to focus fraud risk as a threat priority for cross-border P2P information sharing. The scale of the threat is growing around the world and faster payment systems are increasing the vulnerabilities; yet there is no ‘FATF for fraud’. The current framework for international cooperation, legal clarity in cross-border sharing and the broader protocols for how to receive and act on such risk information – including for restraint and recovery – is inadequate.

The case for improving our response on this front is compelling and there is increasing urgency in the need to act.

We hope this paper can help support policy-makers and industry leaders in that journey and their consideration of the issues. We look forward to supporting those discussions in further research and dialogue activity in this new era.

ENDNOTES

[1] Mexican law also supports information sharing between 'Instituciones de Tecnología Financiera: instituciones de fondos de pagos electrónicos y de financiamiento colectivo' (Financial Technology Institutions: payment and crowdfunding entities), (i) between entities in this same category of payment service provider ; (ii) with foreign and domestic financial entities, and (iii) with financial entities that are members of their Financial Group.
[2] FFIS "Lessons in private-to-private financial information sharing to detect and disrupt crime" (2022) - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf
[3] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version
[4] https://www.future-fis.com/five-years-of-growth-of-public-private-partnerships-to-fight-financial-crime.html
[5] https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf
[6] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Consolidated-FATF-Standards-information-sharing.pdf
[7] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private sector-Information-Sharing.pdf.coredownload.pdf
[8] Paragraphs 80 through 90 in https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private sector-Information-Sharing.pdf.coredownload.pdf
[9] https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html
[10] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7243
[11] https://www.austrac.gov.au/about-us/amlctf-reform/summary-changes-current-regulated-entities#Harm%20prevention%20approach%20to%20tipping%20off
[12] Schedule 5 in https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=LEGISLATION;id=legislation%2Fbills%2Fr7243_aspassed%2F0005;query=Id%3A%22legislation%2Fbills%2Fr7243_aspassed%2F0000%22
[13] See 30 Sep 2024 'Consultation conclusions on information sharing among Authorized Institutions to aid in prevention or detection of crime' https://www.hkma.gov.hk/eng/news-and-media/press-releases/2024/09/20240930-4 and the 'Swiss AML Utility' in the FFIS paper "Lessons in private-to-private financial information sharing to detect and disrupt crime" (2022) - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf
[14] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
[15] Confidentiality of Suspicious Activity Reports, 75 Fed. Reg. 75593, 75590 n. 27 (Dec. 3, 2010), https://www.govinfo.gov/content/pkg/FR-2010-12-03/pdf/2010-29869.pdf
[16] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
[17] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
[18] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
[19] A "financial institution" is defined by FinCEN as referring to any person doing business in one or more of the following capacities:

(1) bank (except bank credit card systems);
(2) broker or dealer in securities;
(3) money services business;
(4) telegraph company;
(5) casino;
(6) card club;
(7) a person subject to supervision by any state or federal bank supervisory authority.

For the regulatory definition of "financial institution," see 31 CFR 1010.100(t) (formerly 31 CFR 103.11(n)).
[20] EXPLANATORY NOTE: Importantly, the BSA does not prohibit financial institutions from sharing information with each other outside of formal channels like 314(b) unless the information is a SAR or would reveal the existence of a SAR. The United States does not have a comprehensive privacy statute that would generally prohibit financial institutions from sharing information with each other. This means that financial institutions may enter into informal sharing arrangements--—including with foreign financial institutions—unless specifically prohibited by applicable law (such as SAR confidentiality, restrictions on access to BOI information filed with FinCEN, or state privacy laws that are not administered by the Treasury or the federal banking agencies). There is no safe harbour from liability for sharing through such informal mechanisms and financial institutions must be satisfied that such mechanisms fall within their own risk tolerance. As discussed above, financial institutions may share information outside of the formal 314(b) channels—including with foreign financial institutions—consistent with applicable law and their own risk tolerance.
[21] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
[22] See Federal Register, Anti-Money Laundering and Countering of Financing of Terrorism Programs, July 3, 2024, https://www.federalregister.gov/documents/2024/07/03/2024-14414/anti-money-laundering-and-countering-the-financing-of-terrorism-programs (citing FinCEN Advisory FIN-2014-A007, "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance," August 11, 2014, at n. 2 ("[i]nformation sharing between financial institutions can often result in a more comprehensive picture of suspicious activity and more useful reporting to law enforcement").
[23] See Federal Register, Anti-Money Laundering and Countering of Financing of Terrorism Programs, July 3, 2024, https://www.federalregister.gov/documents/2024/07/03/2024-14414/anti-money-laundering-and-countering-the-financing-of-terrorism-programs.
[24] FinCEN Director Gacki Encourages Transparency in the U.S. Financial System During International Anti-Money Laundering Conference, March 20, 2024, https://www.fincen.gov/news/news-releases/readout-fincen-director-gacki-encourages-transparency-us-financial-system-during.
[25] FinCEN, OFAC, and FBI Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations, FIN-2023-NTC2, July 16, 2024, https://www.fincen.gov/sites/default/files/shared/FinCEN-Joint-Notice-Timeshare-Mexico-508C-FINAL.pdf.
[26] CHAPTER XIII of the DISPOSICIONES de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito - https://www.gob.mx/cms/uploads/attachment/file/960314/DCG_Bancos_compilado_28.08.2024.pdf

[27] Additional Mexican law also supports information sharing between 'Instituciones de Tecnología Financiera: instituciones de fondos de pagos electrónicos y de financiamiento colectivo' (Financial Technology Institutions: payment and crowdfunding entities), (i) between entities in this same category of payment service provider ; (ii) with foreign and domestic financial entities, and (iii) with financial entities that are members of their Financial Group. This parallel law for FinTechs will be the subject of further analysis by FFIS, but is outside of the scope of this study.
[28] https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023
[29] https://sso.agc.gov.sg/Bills-Supp/11-2023/Published/20230320?DocDate=20230320&ViewType=Pdf&_=20230630204008
[30] https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023
[31] https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic
[32] FFIS *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* (2022) - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf
[33] https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023
[34] https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023
[35] https://www.mas.gov.sg/publications/consultations/2021/fi-fi-information-sharing-platform-for-amlcft
[36] https://www.mas.gov.sg/news/speeches/2023/financial-services-and-markets-amendment-bill-2023
[37] https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628
[38] https://www.mas.gov.sg/regulation/notices/notice-fsm-n02
[39] https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering
[40] https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628#pr6-
[41] FFIS *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* (2022) - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf
[42] https://assets.publishing.service.gov.uk/media/63d270a3e90e071ba44851f9/_f__Information_Sharing_IA_Jan_2023_-_signed.pdf
[43] Paragraph 13. https://www.gov.uk/government/publications/information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act/guidance-on-the-information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act-2023
[44] https://www.gov.uk/government/publications/information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act/guidance-on-the-information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act-2023
[45] https://www.gov.uk/government/publications/economic-crime-plan-2023-to-2026
[46] https://www.gov.uk/government/publications/information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act/guidance-on-the-information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act-2023
[47] https://www.gov.uk/government/publications/information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act/guidance-on-the-information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act-2023
[48] Paragraph 17 of https://www.gov.uk/government/publications/information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act/guidance-on-the-information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act-2023
[49] Paragraph 15 of https://www.gov.uk/government/publications/information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act/guidance-on-the-information-sharing-measures-in-the-economic-crime-and-corporate-transparency-act-2023
[50] All references to the AMLR Article 75 relate to Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L, 2024/1624, 19.6.2024
[51] These Articles are:

[Identification of third countries with significant strategic deficiencies in their national AML/CFT regimes] Article 29,
[Identification of third countries with compliance weaknesses in their national AML/CFT regimes] Article 30,
[Identification of third countries posing a specific and serious threat to the Union's financial system] Article 31
[Specific enhanced due diligence measures for cross-border correspondent relationships] Article 36
[Specific enhanced due diligence measures for cross-border correspondent relationships for crypto-asset service providers] Article 37
[Specific measures for individual third-country respondent institutions] Article 38
[Prohibition of correspondent relationships with shell institutions] Article 39
[Measures to mitigate risks in relation to transactions with a self-hosted address] Article 40
[Specific provisions regarding applicants for residence by investment schemes] Article 41
[Specific provisions regarding politically exposed persons] Article 42
[List of prominent public functions] Article 43
[Politically exposed persons who are beneficiaries of insurance policies] Article 44
[Measures for persons who cease to be politically exposed persons] Article 45
[Family members and persons known to be close associates of politically exposed persons] Article 46 of this Regulation

[52] This is referenced in AMLR as including options such in the transposing Directive (EU) 2016/680 #and with the applicable provisions of national criminal procedural law, including prior judicial authorisation or any other national procedural safeguard as required.
[53] At the time of research cut off (6 January 2025) proposed regulations have been published through the 'Canada Gazette, Part 1, Volume 158, Number 48: Regulations Amending the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations and the Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations.' The requirements in the pre-published Regulations could be amended further based on submissions received during the consultation period and ahead of final publication.
[54] FFIS (2022) *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf
[55] See FFIS (2022) *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf
[56] https://gdprhub.eu/Article_6_GDPR
[57] See P9_TA(2024)0298

Payment services in the internal market and amending Regulation (EU) No 1093/2010
European Parliament legislative resolution of 23 April 2024 on the proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD))

[58] LIC Article 115 Bis is complementary to LIC Article 52, which refers to Anti-Fraud information sharing mechanism. Likewise, the Circular Única de Bancos (CUB) "Bank's Rules" from CNBV, was amended in 2024 in order to make mandatory the Anti-Fraud information sharing among Mexican Banks.

[59] The potential of privacy enhancing technology is explored in more detail in FFIS (2021) *"FFIS Innovation and discussion paper: "Case studies of the use of privacy preserving analysis to tackle financial crime"* Version 1.3. (January 2021)

[60] FNA (2024) "Preserving Data Sovereignty in National Fraud Portals - a Distributed Data Architecture" (FNA Papers: No. 9)

[61] These governance issues are explored in detail in FFIS (2022) *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf

[62] https://www.eba.europa.eu/eba-alerts-detrimental-impact-unwarranted-de-risking-and-ineffective-management-money-laundering-and

[63] Paragraphs 80 through 90: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private sector-Information-Sharing.pdf.coredownload.pdf

[64] See FFIS 2024 'The case for the G20 cross-border payments reform 'Roadmap' to embed economic crime security by design' - https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_-_payments_policy_discussion_paper_2_-_g20_payments_roadmap_and_economic_crime_security__.pdf

[65] https://web-archive.oecd.org/tax/automatic-exchange/common-reporting-standard/index.htm

[66] https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf

[67] https://www.coe.int/en/web/cybercrime/the-budapest-convention

[68] https://www.mha.gov.sg/mediaroom/speeches/regional-anti-scam-conference-2023/

[69] https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit

[70] Bank for International Settlements, *"Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders"* (31 May 2023) https://www.bis.org/publ/othp66.htm

[71] https://www.fatf-gafi.org/en/the-fatf/ministerial-declarations.html

[72] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

[73] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-public-consultation-Feb24.html

[74] Section 2 of FATF *INTERPRETIVE NOTE TO RECOMMENDATION 16 in "The FATF Recommendations"* (February 2023), p17 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations

[75] In the revised changes to R16 there is no support to enabling tracing, but the focus is on screening capabilities https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R.16-public-consultation-Feb24.html

[76] Bank for International Settlements (May 2023) *"Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders"*, p55 https://www.bis.org/publ/othp66.htm

[77] https://www.future-fis.com/lessons-in-private-private-financial-information-sharing-to-detect-and-disrupt-crime.html

[78] Vocalink presentation to Europol Financial Intelligence Public Private Partnership (EFIPPP) Innovation Working Group (IWG) meeting focused on *"Payments analytics - Building capacity and a community of practice in Europe and beyond"* (The Hague) [11 April 2023] with reference to Vocalink *"Trace Financial Crime"* Financial Crime Solutions pdf (June 2022) p15

[79] Pay.UK presentation to *"Data Connectivity and 'Whole of System' Thinking in the UK's Architecture to Tackle Economic Crime"* FFIS Roundtable (London) [2 May 2023]

[80] https://www.bnm.gov.my/-/nfp-launch

[81] Research submission by FNA on 'Case study: FNA Money Trails at Malaysian National Fraud Portal' November 2024

[82] https://www.fsb.org/2023/10/g20-roadmap-for-enhancing-cross-border-payments-consolidated-progress-report-for-2023/

[83] https://www.fsb.org/2023/02/g20-roadmap-for-enhancing-cross-border-payments-priority-actions-for-achieving-the-g20-targets/

[84] Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments: Final report - https://www.fsb.org/2024/12/recommendations-to-promote-alignment-and-interoperability-across-data-frameworks-related-to-cross-border-payments-final-report/

[85] https://www.fsb.org/2024/07/recommendations-to-promote-alignment-and-interoperability-across-data-frameworks-related-to-cross-border-payments-consultation-report/ (page 4)

[86] https://www.fsb.org/uploads/P121224-1.pdf

[87] https://www.fsb.org/2024/07/recommendations-to-promote-alignment-and-interoperability-across-data-frameworks-related-to-cross-border-payments-consultation-report/ (page 17)

[88] https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf

[89] https://www.coe.int/en/web/cybercrime/the-budapest-convention

[90] Article 31. Under 'Freezing, seizure and confiscation of the proceeds of crime', paragraph 2 states that "Each State Party shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any [proceeds of cyber-crime] for the purpose of eventual confiscation."

[91] Article 53. Under 'Preventive measures', paragraph 1 states that "Each State Party shall endeavour, in accordance with fundamental principles of its legal system, to develop and implement or maintain effective and coordinated policies and best practices to reduce existing or future opportunities for cybercrime through appropriate legislative, administrative or other measures." And, in paragraph 2, that "Each State Party shall take appropriate measures, within its means and in accordance with fundamental principles of its domestic law, to promote the active participation of relevant individuals and entities outside the public sector, such as non-governmental organizations, civil society organizations, academic institutions and private sector entities, as well as the general public, in the relevant aspects of prevention of the offences established in accordance with this Convention." Paragraph 3 highlights that "Preventive measures may include: (a) Strengthening cooperation between law enforcement agencies or prosecutors and relevant individuals and entities outside the public sector, such as non-governmental organizations, civil society organizations, academic institutions and private sector entities for the purpose of addressing relevant aspects of preventing and combating the offences established in accordance with this Convention" and, crucially, "(m) Preventing and detecting transfers of proceeds of crime and property related to the offences established in accordance with this Convention."

[92] Article 57. Provides for the forming of a 'Conference of the States Parties to the Convention' to "improve capacity of and cooperation between States Parties to achieve the objectives" of the Convention and that such a conference should take place not later than one year following the entry into force of the Convention and, thereafter, that regular meetings of the Conference shall be held.
[93] www.future-fis.com
[94] https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628
[95] FinCEN Director Gacki Encourages Transparency in the U.S. Financial System During International Anti-Money Laundering Conference, March 20, 2024, https://www.fincen.gov/news/news-releases/readout-fincen-director-gacki-encourages-transparency-us-financial-system-during.
[96] FinCEN, OFAC, and FBI Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations, FIN-2023-NTC2, July 16, 2024, https://www.fincen.gov/sites/default/files/shared/FinCEN-Joint-Notice-Timeshare-Mexico-508C-FINAL.pdf.
[97] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private sector-Information-Sharing.pdf.coredownload.pdf
[98] https://www.future-fis.com/five-years-of-growth-of-public-private-partnerships-to-fight-financial-crime.html
[99] https://assets.publishing.service.gov.uk/media/5eb413f3d3bf7f5d3c74a2b2/Corporate_Group_Cross-Border_Sharing_-_public_statement_for_publication.pdf
[100] See Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies, January 20, 2006, https://www.fincen.gov/sites/default/files/guidance/sarsharingguidance01122006.pdf.
[101] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849
[102] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849
[103] https://assets.publishing.service.gov.uk/media/5eb413f3d3bf7f5d3c74a2b2/Corporate_Group_Cross-Border_Sharing_-_public_statement_for_publication.pdf
[104] https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf
[105] https://petsprizechallenges.com/
[106] https://www.bis.org/about/bisih/topics/fmis/aurora.htm
[107] https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html
[108] All references are derived from the case study launch materials https://www.swift.com/news-events/news/harnessing-ai-fight-against-payments-fraud; https://www.swift.com/news-events/press-releases/swift-and-global-banks-launch-ai-pilots-tackle-cross-border-payments-fraud, supplemented by a research interview process between Swift experts and the FFIS research programme
[109] For example, https://www.microsoft.com/en-us/ai/principles-and-approach