Future of Financial Intelligence Sharing (FFIS)

A Survey and Policy Discussion Paper:

"Lessons in private-private financial information sharing to detect and disrupt crime"

July 2022

RUSI
www.rusi.org

FFIS
Future of Financial Intelligence Sharing

A Survey and Policy Discussion Paper:
"Lessons in private-private financial information sharing to detect and disrupt crime"

25 July 2022

Abstract

This paper surveys international developments in forms of information sharing between private sector entities to detect economic crime risk, covering both fraud prevention and anti-money laundering (AML) domains of economic crime. Through a survey and workshop process which ran from mid-2021 to June 2022, this study draws out detailed reference information about 'platforms' for private-to-private sector financial information sharing from across the UK, the Netherlands, the United States, Singapore, Estonia, Switzerland and Australia.

Section 1 of this paper sets out the background for why private-private sharing is a topic of interest in considering the effectiveness of economic crime detection systems and the rationale for this study exploring both fraud prevention and AML together. **Section 2** provides further background information by summarising the legislative basis for private-private economic crime-related information sharing in the U.S. and the UK.

Section 3 presents the survey results of 15 different 'platforms' and describes how they vary in terms of the capabilities they offer, the data they ingest and provide back to members, the legal framework they operate in, what impact or performance information they record, how they engage with public authorities, how they communicate with data subjects and what interaction they have with financial exclusion issues.

Section 4 provides summary analysis which observes: (1) that private-private financial information sharing platforms are having a demonstrable impact in detecting economic crime risk; (2) that significant strides forward have taken place in resolving data inter-operability issues between private-sector entities so as to link respective datasets; and (3) that the EU General Data Protection Regulation (GDPR) is, prima facie, not a barrier to such platforms operating. However, the paper also observes that many of the platforms are stymied by an unclear policy and regulatory environment that does not provide for a specific enabling legal basis for the information-sharing, contributing to various limiting effects. This section argues that the rise of private-private financial information-sharing platforms presents capabilities for policy-makers (and society at large) to address economic crime. However, the paper argues that the use of these capabilities will remain sub-optimal when the overall policy framework is unclear or contradictory on key issues relevant to the use of such capabilities. The section highlights that a principal challenge is that, in most countries and at the level of international standards, there is no policy consensus on whether financial exclusion of high-risk entities is the desired objective of the system or not. In concluding remarks, this paper suggests that it is incumbent on policy-makers to be more precise about their intended policy objectives in terms of detection, support to law enforcement investigations, asset recovery or financial exclusion and ensure that the overall policy and regulatory framework encourages the information-sharing necessary to achieve the desired outcomes.

Section 5, the final section of the study, is intended as a guide for policy-makers. It sets out three enabling themes and 15 key contributing factors which aim to serve policy consideration about how to support the growth of private-private financial information-sharing capabilities in a secure, effective and efficient manner that meets both data protection and economic crime policy needs.

About

This paper is produced by the Future of Financial Intelligence Sharing (FFIS) programme, as part of our mission to lead independent research into the role of public-private and private-private financial information-sharing to detect, prevent and disrupt crime. The FFIS programme is a research partnership within the RUSI Centre for Financial Crime & Security Studies.

Founded in 1831, the Royal United Services Institute (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 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 research paper and our broader research programme. The FFIS programme is grateful for our strategic research and events partners in 2021/22: Deloitte, Western Union, Chainalysis, Oliver Wyman, Refinitiv and Verafin. We are delighted that this research paper has been supported by Synectics Solutions and supplemented by grant funding by the SWIFT Institute.

We also would like to thank project managers, senior directors and founders from across the 15 private-private financial information-sharing platforms surveyed in this paper who have been involved in the interview and workshop research process.

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 of economic crime.

All information in the survey Section was believed to be correct by the author as of 31 January 2022. 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.

25th July 2022
Author: Nick Maxwell

Reference citation: *Maxwell, N (2022). A Survey and Policy Discussion Paper: 'Lessons in private-private financial information sharing to detect and disrupt crime'. Future of Financial Intelligence Sharing (FFIS) research programme.*

Contents

Executive Summary

The threat of economic crime is severe and unabating. A fundamental challenge to delivering an effective response to that threat is the sharp contrast between how economic criminals can collaborate and network themselves and the corresponding limitations in information-sharing and collaboration across parties and agencies who have a responsibility to protect the system.

Economic crime is typically undertaken through networks of accounts that span multiple financial institutions and jurisdictions. However, historically, detection and investigation of economic crime has been stymied by analytical efforts being siloed and fragmented on many levels, including:

- **At the level of individual private sector institutions.** Primary responsibility for identifying economic crime risk is highly dispersed and fragmented across individual private sector institutions or regulated entities.
- **By business sector.** Where industry initiatives to coordinate a response to economic crime threats do exist, they can often be siloed within a specific business, industry or financial sector.
- **Between public and private sectors.** Despite strong growth in public-private financial information-sharing partnerships in the 2010s, there are still substantial silos of public and private sector activity to disrupt economic crime and lack of connected data relevant to analysis of threats.
- **Between domains of economic crime.** At the international level, the national level and even within individual financial institutions, different domains of economic crime – fraud, money laundering or cyber-enabled economic crime – are often managed separately, with limited cross-over in analytical processes, despite evidence of the links within underlying criminality.
- **Across borders.** Both private sector and public sector efforts to detect and investigate economic crime are significantly impeded at the cross-border level by limits of jurisdiction and information-sharing.

Since 2017, the FFIS programme has published a large body of work exploring the role of public-private financial information-sharing partnerships, primarily at the national-level, and charted the considerable growth of such partnerships around the world since 2015.

In this study, for the first time, the FFIS programme provides an international comparative survey of private-private information-sharing platforms (i.e. information sharing primarily occurring between private sector entities) that are intended to support the detection and investigation of economic crime.

The scope of this work includes both initiatives that are centred on fraud and those which are primarily focused on money laundering threats, and – indeed – those platforms which support sharing across both those domains of economic crime.

Private-private economic crime-related information sharing holds a promise to deliver a number of advantages, including:

- To support analysis over a much broader data sample than is possible when regulated entities conduct analysis in silos;
- To allow for observation of risk, spanning multiple entities, that individual entities would not otherwise be able to detect;
- To reduce duplication in the discovery of risk by sharing investigative insights observed by individual regulated entities;
- Thus, to achieve an earlier awareness of risk and earlier action to mitigate that risk;

- In some cases, to operate in real-time, or close to real-time, and at a greater scale in terms of the number of cases, compared to public-private financial information-sharing partnerships;
- To involve a larger number of regulated entities or other private sector parties, compared to public-private partnerships;
- To be centred on digital processes and data connectivity;
- To support large data analysis and - in some cases - advanced machine-learning capabilities;
- To allow for much more effective discovery of 'unknown-unknowns' (compared to public-private information sharing) as well as enriching the picture of 'known-unknowns' to law enforcement;
- To mitigate the challenge of continual risk displacement of illicit funds around the financial system, caused by individual regulated entities acting in isolation to expel risk from their own business; and
- To achieve more comprehensive and consistent preventative action against high-risk entities across the financial system.

This study surveys 15 different private-private economic crime-related platforms, covering activities and initiatives in the United States, the United Kingdom, Singapore, the Netherlands, Switzerland, Estonia and Australia.

As a result of our study, we observe a highly diverse landscape of different capabilities and different approaches to key design questions being deployed in private-private information-sharing platforms.

Ultimately, we observe a nascent and under-developed policy landscape in support in private-private economic crime-related information sharing.

The survey identified that:

i. Various capabilities are being demonstrated by platforms - from data-driven development of economic crime typologies, to transaction monitoring, to adverse databases, to joint investigations, to messaging capabilities.

ii. Platforms vary significantly in their maturity and history of operations; from being decades-old established utilities, to being very recently established technology platforms or joint ventures between financial institutions, to pilots and proofs of concept.

iii. Fraud prevention has a much longer history as a domain of private-private information sharing, compared to AML.

iv. However, AML private-private information-sharing platforms have significantly expanded in number since 2020.

v. A substantial number of platforms support both AML and fraud information sharing, though many are specialised in one respective domain.

vi. The legal form of the platform can vary from non-profit, to for-profit, to a non-commercial public agency-led initiative.

vii. The lead organising party in the platform can vary significantly – from public agencies, to a technology platform, to financial institutions, to industry associations.

viii. Public agencies are sometimes playing a significant role in activities which are, essentially, private-private information-sharing capabilities.

ix. The role of the platform can vary from having full visibility over underlying data, to having no visibility.

x. More recent platforms are deploying privacy enhancing technologies, which allow for computational results to be shared without having to share or pool raw data for analysis.

While performance data and performance management processes remain embryonic in many cases, available data and key stakeholder interviews indicate that private-private information-sharing platforms are achieving substantial results, including:

- Platforms have demonstrated that large amounts of data can be inter-connected and processed securely and efficiently.
- Platforms have recorded billions of USD dollars / GBP sterling in loss to fraud being prevented.
- Platforms can illustrate improved detection rates of financial crime risk and greater discovery of subjects of interest;
- Platforms are supporting a faster speed of response and time-saving compared to more traditional processes;
- Platforms observe a reduction in the propensity for criminals to target participating institutions;
- In some cases, platforms can link their work to recovery of funds, relevant to financial crime risk;
- Platforms can help reduce duplication of processes and cost by allowing resources and analytical effort to be pooled; and
- Platforms can reduce the risk displacement effect, whereby an 'exited' customer for financial crime risk reasons is merely displaced to another financial institution.

Our survey highlights that a key variable for platforms is what capability they deliver for members, what input data they require and what visibility of the data they have. Some platforms operate with broad transactional data and others with only alerted data. Some platforms have full visibility over the input data and some have no visibility over the input data. This has wide ranging implications for the capabilities of the platform and the interaction with data protection considerations.

Other key variables with notable differences in practice highlighted in this survey include:

- What type of input data is involved;
- How public agencies are engaged in the platform analysis;
- Whether the data centralised or decentralised and what privacy preserving technology is used;
- Who determines economic crime risk that is communicated to members (the platform or other members);
- Whether or not the platform generates intelligence on new typologies of crime;
- The legislative basis to enable the information-sharing through platforms and whether there is a specific enabling clause for the respective information-sharing or platform;
- Whether protection from liabilities exists in the process of information-sharing;
- Whether participation is voluntary or mandatory;
- The information-security standards that are required; and
- Whether cross border information sharing is permitted.

Concerns around financial exclusion are a significant, if not a primary policy concern, when it comes to assessing negative or unintended consequences of enhanced private-private AML/CFT information-sharing.

While it is the purpose of the AML/CFT regime to deny 'illicit funds' access to the financial system, it is not clear that there is a policy consensus in most countries that citizens should be consistently excluded from financial services on the basis of a financial crime risk assessment and outside of a judicial process.

Operating within this somewhat confused policy environment, private-private sharing platforms have adopted a range of different approaches.

Some platforms engage directly with the data subject to inform them of inclusion in the platform, while – for others – this is prohibited through 'anti-tipping off' provisions. Only a small minority of platforms provide clear and explicit support to a data subject who is seeking data correction. For a number of platforms, it is unclear how a data subject could effectively challenge the validity of assessments and the accuracy of information held on the platform.

Beyond the thorny issue of financial exclusion, we raise three 'enabling themes' and 15 contributing factors to further develop and support the growth of information-sharing platforms and address current challenges.

We argue that the future development and effectiveness of private-private economic crime-related platforms can be supported by being:

1) Encompassed within a **shared strategic vision** between public and private sector stakeholders for how economic crime is addressed, with clarity about the respective function and information-sharing requirements of both public and private sectors. This vision should include an overall commitment to data connectivity, it should recognise the extent of capacity of law enforcement engagement to respond to the threats and address how the remaining threats should be handled, it should take responsibility for how subjects of concern should be treated (including clarity over the use of financial exclusion as an objective), and should be underpinned by joint strategic communication endeavours to promote public acceptance and a 'social licence' for the platforms to operate.

2) Delivered through a **clear enabling legislative and regulatory environment,** with both a policy commitment to achieve legal clarity on the required information sharing and supervisory clarity that such information-sharing is permissible and desirable (taking into account data protection, competition law, civil damages and AML regulatory regimes).

3) Developed with a framework of **good governance, data ethics and accountability,** including sustainable funding, attention to cyber security risks, adequate information security standards, operating procedures and professional standards, appropriate use of technology to enable information-sharing and a robust approach to data ethics, with due regard to privacy protection and the potential for analytical bias. The framework should be accompanied with transparent performance reporting and accountability.

Most jurisdictions have some level of private-private information sharing on economic crime risk; which may be as simple as informal meetings allowing financial institutions to share views on trends and typologies. However, this study highlights the impact of - and legal and policy considerations that are relevant when - customer data can be shared between private sector entities. For AML activity, this field of innovation is still in its infancy and the growth in AML information sharing platforms since 2020 is occurring in only a handful of jurisdictions and where there has been clear policy and legislative support provided to such activity.

Ultimately, private-private collaboration platforms provide policy makers – and society at large – with additional capabilities to achieve a public interest goal of fighting economic crime. The three themes and 15

enabling factors set out in Section 5 of this report aim to provide a guide to policy-makers as they determine how they wish such capabilities to be deployed in their countries.

Through private-private collaboration platforms, it is possible to achieve more consistent financial exclusion decisions against high-risk entities. It is possible to support real-time identification and interdiction of the proceeds of crime flowing across multiple financial institutions – and even across borders. It is possible to re-orient the AML framework from being focused on collecting a vast record of historic suspicious transactions, to being an intelligence-led public-private and private-private collaborative effort to dismantle crime networks.

Whether this is desirable or not, is – principally – a matter for policy and public debate. Enabling technology and innovation exists, but the private sector cannot solve these broader policy questions by themselves.

This paper is primarily intended to provide a basis for further engagement with policymakers, supervisors and both private sector and public sector leaders involved in attempting to respond to economic crime threats. We hope this paper is a useful reference document and will support consideration, feedback and the sharing of insight in relation to private-private collaboration to detect economic crime risk.

Research objectives

The objectives of this project are to draw together international experience with regard to private-to-private sector financial information sharing to detect and disrupt crime (across fraud and anti-money laundering domains).

The process is designed to support, in particular, the UK, legislative and policy reform process relevant to expanding the legal gateway for private-private AML information sharing.

The study includes case studies from the following countries: the United Kingdom; the United States; Singapore; Australia; The Netherlands; Estonia; and Switzerland. The research questions guiding this study are:

a) **Describing the current landscape:** What legal provisions and operational solutions exists to support private-private financial information sharing, with regard to both fraud prevention and anti-money laundering?

b) **Identifying the impact of existing private-private sharing:** What impact has been achieved and recorded in crime identification and disruption through existing processes? What limitations do practitioners observe in terms of the effectiveness of current processes; considering identification, disruption and prevention of crime outcomes?

c) **Exploring legal or policy barriers and other adoption considerations:** What legal or policy issues present barriers to the effectiveness of current approaches, including lack of clarity in relevant legal frameworks and the coherence with data privacy or competition-law requirements? More broadly, what technical, governance or ethical issues are relevant to the wider adoption of private-private financial information sharing?

Setting out recommendations for policymakers and private sector leaders. The paper is to propose recommendations for policymakers and private sector leaders to consider opportunities for action and to respond to challenges identified in the field of private-to-private financial information sharing to tackle economic crime.

Methodology

Research process. This paper is the product of:

- Open-source research/literature review of relevant material;
- A survey process covering individual private-private sharing platforms;
- Interviews with key stakeholders involved in respective private-private sharing initiatives;
- 4 principal project workshops and a number of smaller virtual roundtables and discussion events to discuss the operation of respective private-private information-sharing platforms;
- International comparative analysis of the various attributes associated to the private-private information sharing platforms, including the legal basis, measures of activity and outcomes, nature of data sharing, engaging with data subjects and data protection considerations; and
- Feedback and peer-review on draft versions of the study.

The primary research cut-off period was 31 January 2022 and information should only be taken to be accurate and correct at that time, unless otherwise stated.

Definitions

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'[1], 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 is used to provide a holistic response to the following types of criminality:

- fraud against the individual, private sector and public sector
- terrorist financing
- sanctions contravention
- market abuse
- corruption and bribery
- the laundering of proceeds of all crimes
- The recovery of criminal and terrorist assets is also in scope.

In terms of sectoral coverage, the paper is primarily concerned with the major financial institutions, including banking, money service business and insurance sectors. However, the study also explores briefly the role of non-traditional sectors in the economic crime space – such as technology/social media companies and telecommunications companies (TELCOs).

This study seeks to draw from experience in two main domains of economic crime, i.e. money laundering and fraud. We also make reference to cyber security threats as a related domain, but this study does not provide a detailed review of cyber-related information sharing platforms.

As a result, for the purposes of terminology within this study, we primarily refer to the following:

- AML-domain information-sharing;
- Fraud-domain information sharing; and
- Economic crime-related (ECR) information sharing (which refers to coverage of both AML and fraud domains collectively).

In academic literature, fraud - in particular - suffers from a lack of consensus around a definition, including what activity constitutes fraud and where the boundary (and overlap) is between fraud and money laundering or other crimes.

We do not seek to resolve these definitional issues in this study. When we categorise activity as occurring within the fraud-domain or AML-domain respectively, we generally rely on how the relevant platform has self-referred to the activity or by reference to the legislation under which the activity is authorised.

Fraud is generally considered to be a predicate crime, the proceeds of which can then be laundered. However, there are examples where the divide is less clear – such as in the act of being a 'money mule', which can be considered both an act of money laundering and a fraud against the financial institution at the same time. The money mule may have committed fraud in the setting up of the account and the act of money laundering through the account may also constitute a fraud if activity has been mis-represented or accompanied with false documentation to the financial institution. Money laundering, more broadly, may require a criminal party to make fraudulent claims, mis-represent facts or mis-use of a facility of the financial institutions. The inter-relationship between these fields of economic crime and the latest evidence of the overlap in the use of these criminal practices by the same criminal parties is explored later in this study.

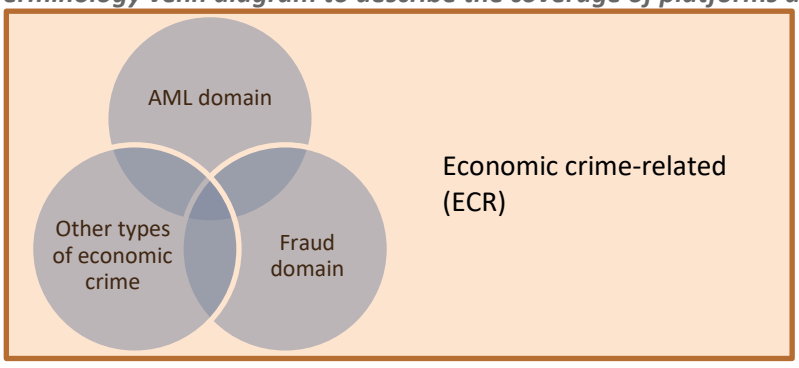
In this study we refer to "platforms" to mean any process, organisation, technology solution or data intermediary that allows for information relevant to the detection or investigation of economic crime to be shared between two or more members (typically financial institutions) of the platform.

Following our terminology from previous FFIS studies, we refer to "partnerships" as shorthand for public-private partnerships, which involved information sharing between public agencies and private sector entities for the purposes of detecting or investigating economic crime.

In cases where legislation allows for an aspect of ECR information-sharing between private sector entities, but the interaction between the two parties is direct, bi-lateral and does not involve an intermediary, we consider this use of a "legal gateway" for information sharing without use of a "platform".

We differentiate between AML platforms and fraud platforms if the platform is normally limited in purpose to processing data relevant to just one of those respective domains. Such restriction could be due to the wording of relevant legislation (that imposes a specific purpose limitation for instance), a self-reported purpose limitation, or simply a limitation evident from historic use of the facility. Such limitations may not necessarily reflect an absolute restriction on operating in an alternative or additional ECR domain in the future.

Terminology venn diagram to describe the coverage of platforms analysed in this study.



In some cases, we use the term 'transaction monitoring' to refer to broader processes of analysing data that has not already been 'alerted' for economic crime risk. In the case of the insurance sector, this analysis or monitoring of general 'transactional data' can refer policy or claim data; i.e. 'non-alerted' customer data.

SECTION 1 – Exploring the basis and fundamentals of private-private information sharing to disrupt economic crime

1.1. Why are we interested in private-private information sharing?

According to FATF, 'effective information-sharing is [a] cornerstone of a well-functioning [anti-money laundering and counter terrorist financing] AML/CFT framework'.[2] Under the FATF international standards, AML/CFT regimes are based on a set of legal and supervisory obligations for financial institutions and other private sector service providers to proactively identify and report suspicions of the laundering of criminal proceeds and/or the facilitation of terrorist financing to government Financial Intelligence Units (FIUs). In order to produce these suspicious activity reports, reporting entities are required to identify suspicion of criminality within their business, using insight that they can develop or procure within their own institution.

Criminals operating professional money laundering schemes[3] can:

- be highly networked;
- adapt rapidly to avoid detection;
- operate internationally with ease;
- conceal their activity across multiple financial institutions; and
- conceal beneficial ownership through layers of legal entities spanning multiple jurisdictions.

Professional money launderers are known to open and manage multiple accounts, across multiple financial institutions.[4] However, the traditional approach to identifying financial crime through national anti-money laundering reporting systems is based on individual financial institutions observing their own business data in isolation from other financial institutions. As such, analysis to identify suspicious activity is taking place on fragmented financial data, with only partial visibility of potential criminal networks.

As the Singapore consultation on financial institution to financial institution sharing puts it:

> *"FIs are not permitted to warn each other about potentially suspicious activity involving their customers. As such, each FI's understanding of their customers' risk profile is limited by the information the FI collects. Criminals have been able to exploit this weakness by conducting transactions through a network of entities holding accounts with different FIs, such that each FI by itself does not have sufficient information to detect and disrupt illicit transactions in a timely manner. Allowing FIs to share information on customers that cross certain risk thresholds enable them to break down these "information silos" and more effectively detect and disrupt criminal activities, reducing any harm done to the integrity of Singapore's financial centre."*[5]

Over a number of years, the FFIS programme has studied the rise of public-private financial information sharing partnerships to respond to the information gaps in the AML/CFT regime.[6] However, the role of information-sharing between regulated entities is a relatively under-explored area of research.

It is conceptually uncontentious that – outside of private-private information sharing – a single regulated entity's understanding of risk will be limited by their siloed view of relevant threats. An ability to analyse networked data derived from multiple financial institutions will have a higher efficacy in detecting risk that spans multiple institutions. However, there are a range of complex policy considerations relevant to the growth of private-private information sharing in the AML/CFT space.

In this study, we draw from insights and examples from a number of countries and highlight potential good practice for AML which has developed in fraud prevention domain, and vice versa.

It is intended that this collation of private-private financial information sharing platforms can constitute a useful reference resource for policy makers and help share knowledge between private-private financial information-sharing platforms about design or policy issues.

1.2. Recent developments in private-private AML/CFT information sharing policy-making

The international standards regime, established through FATF, does not currently provide clear support or direction in terms of the need to establish legal gateways for regulated entities to share AML/CFT risk information between one another.

However, in a major contribution to advancing the international standards engagement with private-private information sharing, in July 2021, FATF - the international standards setter for the AML/CFT regime - published a 'Stocktake on Data Pooling, Collaborative Analytics and Data Protection'.[7]

The study examined how different jurisdictions and initiatives had supported technologies that allow collaborative analytics between financial institutions and other entities, while respecting national and international data privacy and protection legal frameworks. According to FATF, "data pooling and collaborative analytics can help financial institutions better understand, assess and mitigate money laundering and terrorist financing risks. This will make it easier, more dynamic, effective and efficient to identify these activities. It can reduce the number of false positives, enabling the private sector to comply in a timelier and less burdensome manner."[8]

FATF go on to state that "Data sharing is critical to fight money laundering and the financing of terrorism and proliferation. Multinational criminal schemes do not respect national boundaries, nor do criminals or terrorists only exploit one institution to launder their ill-gotten gains or move or use funds with links to terrorism. Customers are increasingly using multiple institutions for banking, instead of banking with a single financial institution with a large market share. This means that data about individual customers is becoming increasingly dispersed across a wide array of financial institutions. If multiple financial institutions share data and apply advanced analytics, it can reveal trends or potentially suspicious activities that could otherwise go undetected by a sole institution."[9]

FATF stated that collaborative analytics can "also help prevent criminals from exploiting the information gaps, as they engage with multiple domestic and international FIs, each having a limited and partial view of transactions."[10] The study examined current practice and also explored potential conflicts with data protection and other individual and fundamental rights. FATF put forward a number of recommendations for national jurisdictions, particularly focused on AML/CFT supervisors and data protection authorities, to strengthen processes that enable technology to enhance collaborative analytics in line with a coherent AML/CFT and data protection policy regime.

FATF call for "Pilot programs, regulatory sandboxes and innovation hubs allow stakeholders to test new technologies for data sharing and analysis, without punitive or overly aggressive regulatory enforcement…. [And] clear guidance from national financial regulators on the kinds of data that could be shared between FIs, and on whether certain technologies (e.g., homomorphic encryption, etc.) and processes enable organisations to remain compliant with national and supranational privacy requirements, in addition to the financial-sector-specific regulations."[11]

Outside of developments at the FATF, a number of jurisdictions have taken significant policy reform steps to consult on and develop private-private information-sharing policy proposals and legislative reforms.

In particular, the Netherlands and UK national action plans place a central emphasis on private-private sharing as part of a broader cross-government and public-private strategy to respond to economic crime threats.

The U.S. has a long standing private-private information-sharing legal regime supported by USA PATRIOT Act section 314(b). However, in 2020/21, the U.S. has undergone massive policy reform with regard the AML/CFT

regime to encourage the regime to be more focused on law enforcement value as a principal outcome and various innovation efforts which are intended to support both private-private and public-private information-sharing.

In October 2021, Singapore launched proposals for a private-private information-sharing platform for AML and counter-proliferation financing (CPF) information-sharing between financial institutions.

	Significant policy-development projects focused on exploring or expanding private-private financial information sharing for the dectection of money laundering risk
	The Netherlands 2019 “Joint Action Plan” on the prevention of money laundering (transaction monitoring and post-suspicion private-private sharing)
	2019-2022 UK Economic Crime Plan (pre-suspicion and post-suspicion private-private sharing)
	The U.S. 2021 Anti-Money Laundering Act and prescribed growth of FinCEN Innovation programmes
	Monetary Authority Of Singapore Consultation Paper on ‘FI-FI Information Sharing Platform for AML/CFT’ October 2021

1.3. How is private-private sharing different to public-private information sharing partnerships?

Since 2015, public-private AML/CFT information sharing partnerships have evolved in numerous advanced economies and financial centres to support a more effective response to AML/CFT threats.

In general, public-private AML/CFT information sharing partnerships support two major types of information sharing and respective outputs:

1. **Strategic intelligence sharing.** Public and private members of the partnership co-develop typologies or knowledge products covering financial crime threats and highlighting relevant behavioural indicators. Typically, these products do not contain confidential identifying information about specific suspects or entities, or individual clients or customers of financial institutions and, as such, do not require enabling legislation. It is generally intended that these knowledge products are made available to non-members of partnerships and are either published and accessible online (such as in the US or in Singapore), or are released through non-public distribution channels to reporting entities (such as in the UK or Hong Kong).

2. **Tactical information sharing.** Where legislation allows, partnerships have facilitated sensitive information relevant to law enforcement or national intelligence investigations to be shared with reporting entities. This information might include the names of specific individuals, legal entities or other identifying information relevant to a case. Member reporting entities can then use this awareness of priority threats, from the perspective of law enforcement or other public agencies, to search their systems in response to that identified suspicion or indicator. Depending on the legal gateway and format of the partnership, reporting entities can share sensitive information back with law enforcement either through formal reports or dynamically within the partnership.

As highlighted in the 2020 FFIS Survey[12], there are broadly three major types of public-private financial information-sharing partnership format:

1. **Co-location of analysts / Secondment model** – In this format, public and private sector analysts sit side by side, typically in dedicated office space, and work collaboratively in real-time to support partnership objectives. Often, co-located analysts from the private sector are restricted from sharing information that they are exposed to, by virtue of their participation in partnership operations, back with their home financial institution.
2. **Convened meetings with non-permanent membership, at the direction of the FIU** – In this format, the FIU convenes the partnership on an irregular basis with no permanent membership from the private sector. Meetings typically focus on specific cases or financial crime threats, and membership for each meeting or project is chosen in response to the case at hand.
3. **Regularly convened meetings** – In this format, partnership members convene on a regular basis, but do not co-locate for a prolonged amount of time. Participants involved in meetings in this model are typically more senior, than compared to co-location models. In contrast to co-location models, in general, private sector members of regularly convened meetings have the opportunity to share the information, that they receive during the partnership meetings, back to appropriate colleagues in their financial crime intelligence or risk function at their home institution.

Public-private financial information-sharing very often sets out a central role for the government financial intelligence unit or a national law enforcement agency. While a number of private sector-led projects have been developed within public-private partnerships, more common– at least when tactical information sharing

is taking place – is for a project to be initiated by the investigative interests of a public law enforcement or intelligence agency.

In this way, public-private partnerships can be relatively focused on 'known unknowns', i.e. the discovery of additional or connecting information related to existing identifying information of interest to an investigation.

Public-private partnerships can have a number of capacity limitations[13] including:

- A small operational bandwidth for cases;
- A small numbers of private sector members involved, relative to the number of entities that are regulated for AML/CFT purposes;
- Normally dominated by in-person (or virtual) interactions and personal relationships rather than digital processes that can operate at scale;
- Often taking place in addition to, and disconnected from, the main AML/CFT regulatory regime and supervisory process;
- Often reliant on analysis of risk still being undertaken in silos within individual private sector entities before being collated by (typically) a public agency; thereby fragmenting and limiting the efficacy of the initial detection effort; and
- Often taking place with very limited public sector resourcing.

Private-private information sharing holds a promise to deliver a number of advantages, including:

- To support analysis over a much broader data sample compared to regulated entities conduct analysis in silos;
- To allow for observation of connected risk, spanning multiple entities, that individual entities would not otherwise be able to detect;
- To reduce duplication in the discovery of risk by sharing investigative insights observed by individual regulated entities;
- To achieve an earlier awareness of risk and earlier action to mitigate that risk;
- In some cases, to operate in real-time, or close to real-time, and at a greater scale in terms of the number of cases, compared to public-private financial information-sharing partnerships;
- To involve a larger number of regulated entities or other private sector parties, compared to public-private partnerships;
- To be centred on digital processes and data connectivity;
- To support advanced machine-learning capabilities;
- To allow for more effective discovery of 'unknown-unknowns' (compared to public-private information sharing) as well as enriching the picture of 'known-unknowns' to law enforcement;
- To mitigate the challenge of continual risk displacement of illicit funds around the financial system, caused by individual regulated entities acting in isolation to expel risk from their own business; and
- To achieve more comprehensive and consistent preventative action against high-risk entities across the financial system.

Within the AML/CFT framework, the traditional conception of the FIU is that it is the public agency responsible for undertaking analysis of all suspicious reports and providing associated intelligence support to operational agencies.

However, resource constraints severely limit the ability for FIUs to process the reporting it receives. FIUs do not have a live picture of transactions and only operate with the segment of financial behaviour that is observable through a formal filed report.

In contrast to relying on FIU analysis to 'connect the dots' from filed reports, private-private sharing offers:

- The opportunity for a real time understanding of financial behaviour;
- The potential for network wide analytics that capture the complete behaviour of an entity across multiple regulated entities;
- Working from comprehensive data, which is searchable at source, rather than a partial record of historic transactions;
- If coordinated, the ***potential*** for more resources – collectively, in terms of investigating staff and technology – to be applied to support analysis within major regulated entities compared to FIUs.

1.4. Why are we interested in surveying fraud and anti-money laundering information-sharing platforms together?

Historically, fraud and money laundering have been considered in silos within financial institutions and other reporting entities and treated differently from a legal and supervisory perspective. However, there is an increasing trend in industry to consider fraud and money laundering together under a more holistic approach to economic crime – including combining approaches to risk governance and threat assessment across fraud and money laundering (and cyber threats); unifying process controls; and establishing a common incident response approach within financial institutions.[14]

In January 2021, RUSI published a paper on 'The Impact of Fraud on UK National Security'[15] which highlighted the 'nexus' between fraud as a crime type and underlying serious and organised crime groups and terrorist financing operations, setting out the available information across a wide range of fraud techniques – including those deployed against individuals, the State and the private sector.

May and Bina Bhardwa in 2017 found that 'OCGs involved in fraud are considered to have intent and capability across a wider range of areas, including expertise in infiltration, corruption and subversion, as well as involvement in multiple enterprises, good resistance and/or resilience tactics, and access to a ready cash flow'.[16] Law enforcement officers interviewed as part of May and Bhardwa's research estimated that 'the majority, or as much as 90%, of the fraud cases they investigated were committed by OCGs'.[17]

All fraud will likely lead to generation of proceeds of crime and is, therefore, a predicate offence covered by the AML/CTF regime.

Conversely, acts of money laundering can be considered by financial institutions as a misuse of a facility and an abuse of terms and conditions of holding an account. As such money laundering suspicions can fall within activity and information-sharing platforms which are focused on 'fraud' – akin to cases of paying in a false instrument into an account, for example.

As a result of the cross-over and inter-relationship between economic crime threat domains, this study seeks to explore how private-private information sharing platforms vary in their design and what significance the domain of economic crime, whether it be fraud or AML (or both), has in relation to key design factors and relevant policy issues.

SECTION 2 – The legislative basis for private-private information sharing to disrupt economic crime, a deeper look at the U.S. and UK legislative regimes.

2.1. The USA Patriot Act, Section 314(b)

Section 314(b) of the USA PATRIOT Act is the leading international example of a private-private legal gateway for sharing information relevant to AML/CFT investigations.

FinCEN describes 314(b) as a legal instrument that "provides financial institutions with the ability to share information with one another, under a safe harbour that offers protections from liability, in order to better identify and report activities that may involve money laundering or terrorist activities. Participation in information sharing pursuant to Section 314(b) is voluntary, and FinCEN strongly encourages financial institutions to participate."[18] FinCEN goes on to state that Section 314(b) of the USA PATRIOT Act supports financial institutions in:

- 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 overall 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 whose suspicious activities it 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.
- FinCEN also highlight the importance of growing diversity across sectors in the use of 314(b) information sharing; including by broker-dealers and the insurance sector.[19]

On a dedicated 314(b) portal on their website, FinCEN provide the following papers to understand the effectiveness of 314(b) private-private sharing.

- 314(b) Fact Sheet (December 2020)[20]
- 314(b) Infographic: Participation and Reporting (April, 2020)[21]
- 314(b) Infographic: 314(b) References in SARs Suggest Increased Information Sharing (April, 2017)[22]

FinCEN's Fact Sheet of December 2020 clarified that 314(b) is intended by FinCEN to support information-sharing on a wide range of unlawful activity - including fraud and cyber-crimes.[23] However, this is a relatively recent development and, prior to this, 314(b) use had been more traditionally interpretated as a legal gateway for AML/CFT threats and not - necessarily - fraud and cyber-crime threats. This issue of the scope of 314(b) is discussed in more detail in section '3.14' of this report.

2.2. UK policy environment for private-private economic crime related information sharing

In recent years, the UK has emphasised the importance of fostering a strategic cross-government and public-private sector response to economic crime, encompassing both money laundering and wider economic crime threats – including fraud.

In terms of identifying the threat, the UK maintains an estimate that hundreds of billions of pounds of money laundering occur each year.

In relation to Fraud, the government estimates that 40% of all crime committed across the UK is related to fraud.[24] According to the National Crime Agency, "the most robust figures currently available from the Crime Survey of England and Wales reveal there were 3.4 million incidents of fraud in 2016-17… However, we think that fewer than 20 per cent of incidents of fraud are actually reported so the true figure may be much higher. This means that the scale of fraud is very significant, but that under-reporting also hampers our understanding of the threat."[25]

The 2017 Annual Fraud Indicator estimated fraud losses to the UK at around £190 billion every year, with the private sector hit hardest losing around £140 billion.[26] In terms of public sector losses to fraud and error, current estimates indicate that up to £51.8 billion a year is lost. [27]

In its 'Integrated Review of Security, Defence, Development and Foreign Policy', the UK made a policy commitment to enhancing its impact against serious and organised crime, emphasising that more needs to be done to "bolster our response to the most pressing threats the UK faces from organised criminals, including: economic crime, illicit finance and fraud."[28]

Further, the UK Economic Crime Plan 2019-22 sets out a wide range of policy and operational steps to address fraud, corruption and money laundering.[29] A key original priority for the plan was to "pursue better sharing and usage of information to combat economic crime within and between the public and private sectors across all participants". [30]

In May 2021, the UK published an Economic Crime Plan: statement of progress.[31] The paper set out seven additional detailed strategic priorities.

Private-private information sharing is supported through the information sharing provisions in POCA section 339ZB to 339ZG (as inserted by the Criminal Finance Act (CFA)2017). However, in the CFA 2017, the threshold for private-private information sharing was widely believed by regulated entities to be set too high; i.e. at the standard of 'suspicion', whereby a regulated entity will have already met the threshold to file an individual suspicious activity report. As a result, the use of the Criminal Finances Act 2017 mechanism for private-private sharing has been extremely limited since its establishment.

At the time of this research, the UK government is consulting on legislative provisions to "Enabling businesses in the AML regulated sector to more easily share information about activity that could relate to money laundering with other AML regulated sector businesses".[32]

In the context of the UK Economic Crime Plan, a specific cross-government and industry working group has been developing a UK model for 'post-suspicion' economic crime information-sharing, similar to the confirmed fraud information-sharing platform in the UK, to avoid risk displacement when customers are exited by regulated entities.

Focusing on fraud, the UK has a number of specified anti-fraud organisations, established with a legislative basis under section 68 Serious Crime Act 2007. [33] Section 68 provides a power for public sector organisations to disclose information to a specified anti-fraud organisation or otherwise in accordance with arrangements made by such an organisation, for the purposes of preventing fraud or a particular kind of fraud. An anti-fraud organisation is any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes. Article 2 of this Order specifies anti-fraud organisations (SAFOs), which can make use of Section 68 information-sharing powers.

As detailed in section '3.12. What legislative basis enables the information-sharing through platforms?', UK fraud prevention information sharing is generally supported by a legitimate interest basis under GDPR 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."[34]

SECTION 3 – Mapping the international landscape of private-private information sharing to disrupt economic crime

3.1. A survey of private-private financial information-sharing platforms.

In this study we survey 15 private-private financial information sharing platforms (hereafter referred to as 'platforms') and compare the platforms in terms of their design, governance, membership, capabilities, types of data utilised and performance information as self-reported by the platforms. We also seek to understand how the platforms interact with issues of key policy interest – such as financial exclusion and how law enforcement agencies interact with the platforms.

The survey represents the first efforts of its kind to bring together descriptive references for both AML and fraud-domain private-private financial information sharing platforms.

Over the course of the research process, platform managers expressed a view that private-private information sharing (in at least one domain of economic crime) exists to varying degrees in almost all jurisdictions. This may be as simple as an industry association or informal meetings allowing financial institutions to share views on trends and typologies. Within the U.S., bi-lateral information sharing has been possible through USA PATRIOT Act section 314(b) since its enactment in 2001. In this study, however, we are primarily concerned with platforms (of three or more members) that process specific identifying information and personal data about customers and allow the platform, or the members themselves, to better analyse economic crime risk that spans across multiple financial institutions.

As our definition of 'platform' is relatively broad, our current survey is not likely to be exhaustive of platforms in existence. It is our intention to release further updates and include additional private-private sharing platforms in future editions of this paper.

Within this version of the survey, there are 6 UK platform and 9 non-UK platforms.

Private-private financial information sharing platforms	
United Kingdom	**Non-UK**
1. Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) 2. Insurance Fraud Bureau 3. National SIRA – Synectics Solutions[35] 4. UK Finance Fraud Intelligence Sharing Service (FISS)[36] 5. UK Tri-bank initiative 6. Vocalink - Mastercard Trace and Prevent	7. **(United States)** 314(b) Collaborative Investigation Model - a formal association of financial institutions registered under USA PATRIOT Act 314(b) 8. (**United States**) The Duality AML Information Sharing Network in partnership with Oracle 9. (**United States**) Money Services Business Industry Negative Database (MSB-IND) 10. (**United States**) Verafin information sharing, operating under USA PATRIOT Act 314(b) 11. (**Switzerland**) Swiss AML Utility 12. (**Singapore**) COSMIC FI-FI Information Sharing Platform 13. (**Netherlands**) Transactie Monitoring Nederland (TMNL) 14. (**Estonia**) Salv - AML Bridge 15. (**Australia**) Australian Financial Crimes Exchange Ltd (AFCX)

3.2. A timeline of development of AML and fraud domain private-private financial information-sharing platforms.

The platforms surveyed represent a diverse range of models, at very different stages of development maturity and scale. The section below provides a high-level overview of the respective platforms in a timeline of initial establishment of the platform of mechanism.

Date	Platform	Domain
1980 -1989	**(UK) Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) -** Cifas facilitates the sharing of data, intelligence and learning across over 600 organisations from 13 commercial sectors and provides high grade intelligence to enable members to take appropriate risk-based decisions. Cifas provides a searchable database, analytics such as location-based matching, network analysis and proactive alerts and a peer-to-peer messaging platform between members. **[Operational - Not for profit]**	**Fraud**
2000 -2009	**(UK) Insurance Fraud Bureau** - A central hub for sharing insurance-sector fraud data and intelligence; helping UK insurers identify fraud and loss to fraud and supporting police, regulators and other law enforcement agencies in disrupting fraud crimes. **[Operational - Not for profit]**	**Fraud**
	(UK) UK Finance 'Fraud Intelligence Sharing Service' (FISS) - The Information & Intelligence (or 'I&I') Unit within UK Finance - the trade-body for the UK's financial sector - is responsible for the collection, analysis, assessment, alerting and escalation of threats and intelligence impacting the economic crime landscape within the UK financial sector. Through the FISS, UK Finance provide secure, pro-active, open, flexible, centralised intelligence database enabling bulk private-to-private data sharing to support the UK payments industry in fighting fraud. **[Operational - Industry consortium / trade body commercial initiative]**	**Fraud**
	(UK) National SIRA, Synectics Solutions - The largest syndicated database of cross-sector customer fraud risk intelligence in the UK; developed by Synectics Solutions to enable private and public sector organisations to manage risk and prevent fraud; supporting advanced analytics and syndicated access to a wide range of sources of fraud intelligence. **[Operational - Commercial]**	**Fraud**
	(United States) Verafin information sharing, operating under USA PATRIOT Act 314(b) - A registered 314(b) association and leading 314(b) technology platform by membership. As a Nasdaq company, Verafin information-sharing capabilities service an ecosystem of Tier-1 and Tier-2 banks, as well as regulatory authorities and consortium initiatives. **[Operational - Commercial]**	**Both AML and fraud**

2015-2019	**(United States) 314(b) Collaborative Investigation Model - a formal association of financial institutions registered under USA PATRIOT Act 314(b)**. This model allows for a fusion intelligence capability among private sector entities by enabling members to collaborate on investigations spanning multiple financial institutions, working on a common data platform. While primarily focused on case investigations, the model can also support dialogue among members to better understand financial crime trends and typologies. **[Operational - Industry consortium]**	**Both AML and fraud**
	(Australia) Australian Financial Crimes Exchange (AFCX) - A private-private information-sharing platform, exchanging actionable intelligence for the identification, investigation and prevention of financial crimes including fraud and cybercrime. With historic expertise as an adverse database utility for payments fraud incidents, AFCX has ambitions to expand threat coverage and provide real-time intelligence exchange across multiple business and industry sectors and the public sector. **[Operational - Not for profit]**	**Both AML and fraud**
	(UK) Vocalink - Mastercard Trace and Prevent - Vocalink, a Mastercard company, partnered with Pay.UK to develop a world-first, industry-level solution to detect criminal activity across the Faster Payments network. Announced in 2018 and deployed under the name Mule Insights Tactical Solution (MITS), the solution alerts financial institutions to suspect mule accounts within their portfolios, enabling accounts to be investigated. **[Operational - Commercial]**	**Fraud** *(Though, predominantly a money mule focus and, therefore, covering both a fraud and ML threat)*
	(UK) Tri-bank initiative - A UK pilot project to understand if a utility approach to Transaction Monitoring (TM) of Small & Medium Sized Enterprise client data across three large retail banks could enhance members awareness of risk, spanning the membership, whilst respecting appropriate data privacy rules and legislation. **[Pilot, Completed]**	**AML**
2020+	**(Netherlands) Transactie Monitoring Nederland (TMNL)** - A joint venture initiative of five largest banks in the Netherlands to deliver a combined transaction monitoring and alerting capability to achieve more effective detection of patterns and behaviour on a combined transaction dataset. **[Partially operational – Non-commercial enabler]**	**AML**
	(Switzerland) Swiss AML Utility - Multi-bank pilot for collaborative analytics on shared anonymised centralised alerts between participating financial institutions. The data Proof of Concept was completed with anonymised bank data in June 2020. **[Pilot, ongoing]**	**AML**
	(Estonia) Salv - AML Bridge - Fully operational since July 2021, AML Bridge is a secure, auditable and automatable economic crime-related information sharing platform. In 2021, AML Bridge expanded to be adopted by the vast majority of the Estonian banking community and	**Both AML and fraud**

	deployment is planned for three other European markets in 2022. AML Bridge is a key-protected, end-to-end encrypted messaging platform and a member network to share fraud & AML typologies, trends and best-practice solutions. Salv itself does not have access to unencrypted data being shared and only sees metadata and logs of message exchange. **[Operational - Commercial]**	
	(United States) Money Services Business Industry Negative Database (MSB-IND) - Operating under 314(b) as a registered association, this Money Service Business (MSB) sector initiative establishes a utility database for agents who have been 'exited' for financial crime reasons, to prevent re-entry to the MSB market of agents identified as in gross breach of financial crime compliance. **[Operational - Industry consortium]**	**Both AML and fraud**
	(United States) The Duality AML Information Sharing Network in partnership with Oracle – This platform is a privacy preserving, automated query and response capability. This platform enables queries to be submitted to multiple participants at the same time and ensures personal and/or sensitive information is not disclosed within the query. Through the use of privacy enhancing technology, the 'requesting' party does not need to reveal the query to the 'requested' parties. The 'network' can be queried and aggregated responses can be revealed to the requester without necessarily revealing which financial institutions out of the network provided which response. For example, a query focused on exit decisions may provide the requester with information that "3 institutions have exited a customer matching this identifying information for financial crime reasons". For pre-defined and pre-agreed queries, responses can be automatic. The process is designed to achieve information-security benefits, to reduce or remove the requirement to disclose customer data in order to conduct a 314(b) query, to enhance the speed of a response, to 'guarantee' a response and to automate responses. **[Operational / Project Under Development - Commercial]**	**Both AML and fraud**
	(Singapore) COSMIC FI-FI Information Sharing Platform - A Monetary Authority of Singapore (MAS) led initiative, that has been co-created with industry, as a digital platform and enabling regulatory framework for financial institutions to share (between one another) relevant information on customers and transactions to prevent money laundering, terrorism financing and proliferation financing. The new digital platform, named COSMIC, for "Collaborative Sharing of ML/TF Information & Cases", is intended to prevent illicit actors from exploiting information gaps between financial institutions. **[Proposal under consultation - Public agency initiative]**	**AML**

Key takeaways from the timeline of private-private financial information-sharing platform development:

i. Platforms vary significantly in their maturity and history of operations; from being decades-old established utilities, to being very recently established technology platforms or joint ventures between financial institutions, to pilots and proofs of concept.

ii. Fraud prevention has a much longer history as a domain of private-private information sharing.

iii. AML private-private information-sharing platforms have significantly expanded in number since 2020.

iv. A substantial number of platforms support both AML and fraud information sharing, though many are specialised in one respective domain.

v. The legal form of the platform can vary from non-profit, to for-profit, to a non-commercial public agency initiative.

vi. Public agencies are sometimes playing a significant role in activities which are, essentially, private-private information-sharing capabilities.

vii. The lead stakeholders in the platform can vary significantly – from public agencies, to a technology platform, to financial institutions, to industry associations.

viii. The role of the platform can vary from having full visibility over underlying data, to having no visibility.

ix. More recent platforms are deploying privacy enhancing technologies which allow for computational results to be shared without having to share or pool raw data for analysis.

x. Various capabilities are set out - from data-driven development of economic crime typologies, to transaction monitoring, to adverse databases, to messaging capabilities. These capabilities are described in more detail below.

The graphic below illustrates two of the key takeaways that are observable from the timeline of development of private-private financial information sharing platforms, i.e.:

- That fraud information-sharing has a much longer experience as a discipline, with many platforms existing for decades; and
- That, over recent years and months, there has been a substantial growth in AML private-private information-sharing platforms.

Date	Fraud domain platform	Both domains	AML domain platform
1980 -1989	(UK) Cifas		
2000 -2009	(UK) Insurance Fraud Bureau		
	(UK) UK Finance 'Fraud Intelligence Sharing Service' (FISS)		
	(UK) National SIRA, Synectics Solutions		
		(United States) Verafin information sharing, operating under USA PATRIOT Act 314(b)	
2015-2019		(United States) 314(b) Collaborative Investigation Model - a formal association of financial institutions registered under USA PATRIOT Act 314(b)	
		(Australia) Australian Financial Crimes Exchange (AFCX)	
	(UK) Vocalink - Mastercard Trace and Prevent		
2020+			(UK) Tri-bank initiative
			(Netherlands) Transactie Monitoring Nederland (TMNL)
			(Switzerland) Swiss AML Utility
		(Estonia) Salv - AML Bridge	
		(United States) Money Services Business Industry Negative Database (MSB-IND)	
		(United States) The Duality AML Information Sharing Network in partnership with Oracle	
			(Singapore) COSMIC FI-FI Information Sharing Platform

3.3. How do the platforms vary in terms of their coverage of fraud and money laundering risks?

Out of the 15 platforms surveyed, 4 focus on the AML domain, 6 focus on the fraud domain and 5 platforms cover both fraud and AML information-sharing. There is a striking difference in the UK profile of platform domains relative to other jurisdictions. The UK has a relative strength in fraud domain platforms, but a comparative lack of AML private-private information sharing platforms. U.S. platforms stand out for their support to platforms which support both AML and fraud information-sharing.

Private-private financial information sharing platforms	
United Kingdom	**Non-UK**
AML • UK Tri-bank initiative **Fraud** • Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD)[37] • National SIRA – Synectics Solutions • Vocalink - Mastercard Trace and Prevent (Money Mule focus) • UK Finance Fraud Intelligence Sharing Service (FISS) • Insurance Fraud Bureau	**AML** • COSMIC FI-FI Information Sharing Platform • Swiss AML Utility • Transactie Monitoring Nederland (TMNL) **Both fraud and AML** • Salv - AML Bridge • 314(b) Collaborative Investigation Model - a formal association of financial institutions registered under USA PATRIOT Act 314(b) • Money Services Business Industry Negative Database (MSB-IND) • The Duality AML Information Sharing Network in partnership with Oracle • Verafin information sharing, operating under USA PATRIOT Act 314(b) • Australian Financial Crimes Exchange (AFCX)

However, there are numerous definitional challenges in seeking to classify platforms between fraud and AML domains.

Vocalink – Mastercard Trace and Prevent as a platform is focused on money mule activity identification (at the time of this research) which is simultaneously a fraud and a money laundering threat. However, for the purpose of classification within this study, the platform has been defined as a fraud-domain platform as it operates under the basis as if it were a fraud-prevention domain information sharing platform – supported by the 'legitimate interest' basis under GDPR and Recital 47.[38] It should be noted that all fraud domain platforms may be able to address certain money laundering issues, while still being focused (or limited in purpose by legislation) towards fraud prevention activities. This is due to the cross-over in definitions (and definitional challenges) between the two domains of economic crime.

Vice versa, AML platforms may be able to support fraud information sharing despite operating under an AML-focused piece of legislation. As an example, the Salv 'AML Bridge' is considered by its founders to be a use case-agnostic platform that focuses on facilitating the exchange of tactical information – whether that's AML-related, fraud/scam-related, sanctions-related, or other domains of economic crime. While the initial focus for the platform was in the AML domain, Salv has observed that members have increasingly sought to use the platform for fraud/scam related use-cases as well. In 2021, fraud/scam use-cases accounting for 40% of the collaborative investigations conducted through AML Bridge.

3.4. Capabilities

Perhaps the most significant variable for private-private information-sharing platforms is the variance in capabilities and outputs of the respective platforms. In this study we delineate between the following types of capabilities:

A. Development of typologies of economic crime threats.
B. Adverse incident databases.
C. Messaging communication.
D. Combined transaction monitoring.
E. Collaborative intelligence and investigations by members.

Below we summarise various benefits and shortcomings that private-private financial information sharing platforms expressed during interview or presentations in relation to that output.

Development of typologies of economic crime threats.

Much like public-private financial information-sharing partnerships, private entities can share information and co-develop new typologies and indicators of specific crime types. Private-private financial information sharing platforms can also support a data-driven approach to discovering typologies of risk, either through human-centred analysis or forms of machine learning.

While typologies derived from human insight can provide value, they are not considered within this study. This type of human-centric typology sharing is commonplace and occurs in a very large number of forums – i.e. industry association or AML professional conferences and workshops. Given its prevalence, this type of sharing is not covered in this study and, instead, we focus on the practice of (or opportunity for) typological understanding of threats to be developed from shared data within an ECR platform.

Strengths	Typical challenges
Compared to individual members undertaking analysis in silos, ECR platforms have the potential to analyse a greater volume of data (and inter-connected data) to refine models and deploy machine learning techniques over. As a result, typologies of threats should be more accurate and be informed by greater visibility of threats, network connections between high-risk entities and other behavioural indicators which are only apparent in connected data.	Without public sector input it can be difficult to identify typologies of ML, due to the lack of awareness about what behaviour amounts to 'confirmed' money laundering. Without such confirmed incidents it can be difficult to understand 'true positive' indications of risk and also remove 'false positives'. As a result, identification of risk often focuses on anomaly detection.

Relevant features of case studies explored in this study
(United Kingdom) 'Precision' Synectics Solutions applied within National SIRA - Precision, the Synectics Solutions predictive analytics service, is underpinned by an array of machine learning algorithms that can adapt over time to changing fraud techniques. Precision models are recalibrated regularly against outcome data set by members to respond to changing fraud trends and evolving consumer behaviours. Investigative conclusions by members, or 'markings' that investigators set in the course of investigations, are fed back into National SIRA, so that the models can learn over time. Synectics report that R&D is underway to further integrate video, voice & other unstructured data to enhance the anomaly detection capabilities of Precision.

Messaging communication.

Messaging, including single messages but also longer threads of messaging and messaging involving multiple regulated entities in a messaging thread, can provide a powerful capability for ECR investigations. In the U.S., over the majority of its legislative lifetime, the use of USA PATRIOT Act 314(b) has been limited to bi-lateral and direct messaging. Messaging around source of funds for a wire transfer have been cited as a common focus for such messages.

Strengths	Typical challenges or shortcomings
- Can provide counterparty information to either explain behaviour as non-suspicious or further confirm suspicions of economic crime. - Messaging communication can provide the basis for more in-depth information sharing and collaboration, such as joint investigations.	- Respondents can be slow to respond or unresponsive. - Respondents can be concerned about the motivations of requesters (fishing for client information). - Requests can amount to relatively basic and transactional information-sharing on a case-by-case basis and bi-lateral (1:1) basis; not supporting analytical capabilities or broader learning on financial crime risk. - Messaging can be limited to bi-lateral processes and not scalable for multiple entities. - Processes for messaging can be limited to secure email or inefficient processes, in the absence of a platform, adequate technology and data inter-operability. - In the absence of a platform and in the case of bi-lateral messaging, it can be more difficult to respond to governance risks, such as mis-use of information or corrections of data shared.

Relevant features of case studies explored in this study
(United States) Verafin information sharing, operating under USA PATRIOT Act 314(b) - Bi-lateral messaging can be escalated to multi-lateral threads and to collaborative investigations and combined with SAR filing direct from the investigations platform. (Estonia) Salv - AML Bridge - AML Bridge facilitates secure bi-lateral messaging between network members. As the platform host, Salv does not have access to underlying message data and only sees metadata and logs of message exchange. (United States) The Duality AML Information Sharing Network in partnership with Oracle - Communication can be facilitated through privacy preserving technology such that the requester does not reveal the query to the receiver, but the receiver may pre-authorise disclosures of a certain type. Queries are only authorised following an alert within the Oracle AML suite for members." Beyond simplistic messaging, this query process can reveal response from a network at scale and in an automated rapid response framework. The process is decentralised, whereby relevant underlying (sensitive) data does not move and is not disclosed. (Singapore) COSMIC FI-FI Information Sharing Platform - Under the proposed Singapore COSMIC framework, it is envisaged that responses will be compulsory, with responses required to be timely. There will also be criminal penalties for mis-use of the information-sharing facility. A financial institution will be able to share information through COSMIC in three ways, i.e. Request, Provide and Alert. 'Requests' will be permissible when a customer has exhibited some red flag behaviour and a financial institution requires clarification from a counterparty on potential suspicion involving particular activity that the customer has exhibited. 'Provide' will be 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 financial institution would have to proactively provide risk information on the customer to other FIs with a link to the customer's activities. COSMIC 'Alert's are discussed under the 'adverse incident database' capability.

Collaborative transaction monitoring

Collaborative transaction monitoring refers to two or more members (typically financial institutions) pooling, or connecting in a privacy preserving manner, transactions data (or, potentially, only transaction alerts) to be able to analyse risk that spans across multiple financial institutions. Various models are being pursued with respect to this capability – including Financial Intelligence Unit convened models, private sector models that cover all transaction sharing, and pilots that cover only connections of alerted transactions.

A networked view of transactions can illuminate the discovery of chains of payments that are associated to high-risk entities, spanning multiple entities and can allow a more comprehensive picture of financial behaviour to be subject to analysis, thereby improving the efficacy of behavioural analytics and alert generation. Finally, with a network wide transaction data set, both human and machine learning analysis can be enhanced in its potential to discover anomalies.

Members can either analyse directly the network picture or be sent some level of privacy preserving alert to understand whether additional risk exposure for their institution has been identified by the platform.

In some cases, we use the term 'transaction monitoring' to refer to broader processes of analysing data that has not already been 'alerted' for economic crime risk. In the case of the insurance sector, this analysis or monitoring of general 'transactional data' can refer policy or claim data; i.e. 'non-alerted' customer data.

Strengths	Typical challenges or shortcomings
"The whole is more than the sum of its parts" – Aristotle - Compared to a single financial institution attempting to analyse their own data in isolation, a wider network view of transactions enhances the efficacy of detection systems. - Typological analysis or macro-level analysis will be enriched by networked source transaction data. - By tracing payment flows across multiple institutions, intermediary connections to high-risk payment or receiving accounts can be revealed which would otherwise be impossible to observe independently. - Where identifying information on criminal networks can be queried against the networked transaction data, platform members can be alerted to their exposure to such networks.	- The strength of the analysis possible depends on the quality of the source data. - Data-interoperability between multiple financial institutions can be a major technical challenge. - The balance between the analytical value of access to broader and deeper data, must be balanced with data protection principles of data minimisation and purpose limitation and the 'social licence' or public acceptance of such a capability. - Privacy preserving techniques used to enable the collaboration may reduce the opportunity to understand data quality challenges at the platform level. - Privacy preserving techniques used to enable to collaboration may limit utility in the ability to conduct certain types of analysis on certain types of data attributes. - Even at the networked level, to move beyond anomaly detection, transaction monitoring may still require high-confidence information on suspected criminal entities – likely from public agencies.

Relevant features of case studies explored in this study

(UK) Insurance Fraud Bureau

- As a partial equivalent to 'transaction monitoring' in the insurance sector, the (UK) Insurance Fraud Bureau supports analysis on insurance claims/application and policy data (i.e. non-alerted data) through the Motor Insurance Database (MID) and the Motor Anti-Fraud & Fraud Register (MIAFTR). In the UK, there is a legal requirement for insurers to register all vehicle insurance policies into MID as a central database. In addition, insurers can make use of MIAFTR as a voluntary-use claims database (which, while not compulsory, benefits from substantial industry engagement). In addition, the insurance sector can cross check claims against domestic property and personal injury (liability) claims through an industry data exchange called CUE (Claims Underwriting Exchange), which is also voluntary. All of these databases represent non-alerted information which can be analysed to identify risk.

(UK) National SIRA, Synectics Solutions

- Likewise, National SIRA Synectics Solutions can provide members with an intelligence capability to leverage insurance policy and claims data to proactively identify networks of suspicion and provide alerts to members when they have exposure to such a network.

(UK) Vocalink - Mastercard Trace and Prevent

- The Vocalink system essentially supports a form of transaction monitoring but through the UK payments network and has the capability to map payment flows. Vocalink utilise this analytical capability to identify connected accounts to payment flows associated to Mule accounts and to quickly alert financial institutions with exposure to those payment chains.

(UK) Tri-bank initiative

- As a proof of concept, this initiative identified that a utility approach to Transaction Monitoring (TM) of Small & Medium Sized Enterprise client data of three large retail banks could identify risk that was not visible to single financial institutions while respecting data privacy rules and legislation.

(Netherlands) Transactie Monitoring Nederland (TMNL)

- At time of this research, the TMNL platform was operational but limited to analysis business clients' data. Under GDPR, corporate data does not enjoy the same protections as personal data. TMNL supports analysis of business clients' transactions and uses various encryption and privacy preserving techniques to pseudonymise and achieve data minimisation. At the current stage of development, TMNL allows multibank alerts to be generated for participating financial institutions. Note: corporate clients' data at TMNL is classified and treated as personal data.

(Switzerland) Swiss AML Utility

- As a pilot project, the Swiss AML Utility, intermediated by Deloitte AG, is focused on proving value and refining processes and governance structures for further deployment. A restriction in the Swiss AML utility is that only alerted transactions and accounts can be shared. The project has been able to identify the prevalence of the same customer being alerted by different financial institution and to identify new indicators of risk based on the existing data sharing.

Adverse incident databases.

Establishing an adverse incident database has been a major feature of fraud domain initiatives. In the AML domain, there is a greater challenge in reaching a level of awareness of 'confirmed criminality' compared to fraud. However – regardless – adverse incident database capabilities are starting to emerge in the AML context. A trigger for inclusion in AML adverse database, in surveyed platforms, is typically an exit decision by a regulated entity.

Strengths	Typical challenges or shortcomings
- Ensures that risks identified by a single member (or by the platform itself) can be easily accessed and utilised by participating platform members. - Adverse incident databases are particularly useful as protective measures to raise the capability of members to prevent initial access of high-risk potential clients, following a risk-based decision-making process. - Adverse incident databases improve overall efficiencies by reducing the need and cost for members to rediscover the same financial crime risk. - Adverse incident databases normally require robust governance processes to ensure that members do not abuse the facility, that there are opportunities for data subjects to challenge data held on them on accuracy grounds, that standards of information-security and purpose limitation are met.	- Adverse incident databases may be open to challenge in the AML domain due the relative difficulty in assigning a 'confirmed' event of criminality when compared to fraud. - While both private sector investigations of fraud and money laundering will be determining 'suspicion' of an act of criminality, financial institutions will generally have a lower level of confidence in concluding that a money laundering event has taken place, in contrast to a fraudulent event. This can then lead to concerns about the proportionality of sharing such ML-risk information and raise risk of defamation or other litigation by subjects of the ML concern. - Where they exist, AML adverse incident databases tend to focus on client exit decisions by members. - Adverse incident databases may raise risks of financial exclusion.

Relevant features of case studies explored in this study

(UK) Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) and Synectics Solutions (UK) National SIRA

- The Cifas capability and National SIRA platform represent longstanding and successful models that provide multi-sector access to databases and analytics relating to fraudulent conduct. Cifas filings of money mules (as acts of misuse of a banking facility for example), once identified by any given member, can be shared to support risk-based decisions during the on-boarding of a customer by additional financial institutions.

(UK) Insurance Fraud Bureau

- In the case of 'confirmed fraud', IFB members have access to the Insurance Fraud Register, which contains articles such as telephone numbers and email addresses associated to fraud. The grounds for believing that a fraud has taken place is the balance of probability (civil standard) and members have to have made a decision on the basis of fraud, i.e. to repudiate a claim, or to void a policy on the basis of believing it to be a fraudulent event. In this model, the subject of the incident must be contacted and informed that they have been loaded to the insurance fraud database. The process is deliberately designed as an overt process and to support prevention and deterrence of further fraudulent attempts.
- In addition to this the IFB has a 'Suspected Fraud' database (Insurance Fraud Intelligence Hub or IFiHUB) where members can share details of active investigations. The IFiHUB is supplemented with additional intelligence developed by the IBF (including from what it receives from external sources and a public whistleblowing line.

(UK) The UK Finance 'Fraud Intelligence Sharing Service' (FISS)

- Through the FISS, UK Finance provide secure, pro-active, open, flexible, centralised intelligence database enabling bulk private-to-private data sharing to support the UK payments industry in fighting fraud, as submitted by members.

(United States) Money Services Business Industry Negative Database (MSB-IND)

- Operating under authority as a USA PATRIOT Act 314(b) registered association, this initiative establishes a database to record MSB agents that have been exited for financial crime reasons, to prevent re-entry to the MSB market of agents identified as in gross breach of financial crime compliance. This database responds to a longstanding challenge that exited agents could establish themselves with alternative MSB networks after having been exited for financial crime reasons. In this case subjects of the data base are provided with an appeal process prior to being forced to exit an MSB network.

(Singapore) COSMIC FI-FI Information Sharing Platform

- The COSMIC initiative is specifically aimed at mitigating the risk that an exited customer for financial crime reasons from one financial institution can re-enter the Singapore financial system at an alternative financial institution, with no ability of the alternative financial institution to understand the risk as identified by the first financial institution. As such, COSMIC supports an 'Alert' functionality, which essentially establishes an adverse database as a 'watchlist' for customers that have been exited and filed against. The Alert should include the reasons for concern, including red flags observed and relevant risk information on the customer.

  It is planned that the requirement to place a customer on the Alert watchlist will be mandatory.

  Other COSMIC members are not permitted to reject or exit a customer solely based on the fact that the customer is placed on the COSMIC watchlist.

  The proposal within COSMIC also includes a requirement that the financial institution should provide the customer with an opportunity to explain the unusual behaviour and perform its own risk assessment based on the information obtained from the customer, which may provide additional or new perspectives on the risk level of the customer.

  Members of COSMIC will be legally required to rectify and update the risk information of the customer, including the information in the watchlist, where they receive further details that clarify a position or offer explanation to suspicious activity.

Collaborative case investigations by members.

Collaborative case investigations by members involves a shared commitment by multiple private sector entities to pool resources and relevant information on specific cases to support the intelligence development process on criminal networks.

Note: We distinguish here between intelligence capabilities that are developed by a platform independently of the members and where results are dispersed to members as alerts (which we examine under transaction monitoring platform capabilities) and, in this section, we focus on the type of collaboration whereby individual members form joint investigations on shared or pooled data, with data shared via a central platform.

Strengths	Typical challenges or shortcomings
- In this model, members pool and focus investigative resources on specific cases, providing both effectiveness and efficiency benefits compared to investigations in isolation. - The model tends to also feature, or be connected with, strong public-private information sharing with a public law enforcement or investigative agency - both to provide investigative start points and to ensure that the resulting intelligence is actionable by authorities.	- This model can be faced with bandwidth and prioritisation challenges. - Typically, there is no regulatory or supervisory benefit in supporting joint investigations, and so justifying resources to support the process can be challenging for regulated entities. - The model requires critical mass of participating financial institutions.

Relevant features of case studies explored in this study
(UK) Insurance Fraud Bureau - Within the intelligence team at the IFB, if there is enough evidence of organised crime activity with claims against multiple insurers, then the IFB will collaborate with members to present an evidence package to law enforcement. The Association of British Insurers (ABI) fund a dedicated law enforcement unit through the 'fraud levy'. The unit – the Insurance Fraud Enforcement Department (IFED) within the City of London Police – take responsibility for onward investigation of IFB intelligence packages and lead on disruption of the organised crime group. (United States) 314(b) Collaborative Investigation Model - As a formal association operating under USA PATRIOT Act 314(b), the collaborative investigation model frequently leverages public-private information-sharing - via USA PATRIOT Act 314(a) - to receive investigative start points from law enforcement agencies. The members of this model can then pool their investigative resources to 'supercharge' an investigation. Members build out a greater understanding of a network of criminality from the initial starting point provided by law enforcement or members' own subjects of interest. This model has been applied to cases relevant to corruption, cybercrime and security, foreign and domestic terrorist financing, fraud, transnational organised crime, drug trafficking, human trafficking, illegal wildlife trade and proliferation finance. Information shared in this model is targeted for specific case investigations, not to support an adverse incident database or joint transaction monitoring.

Table - Overview of platform capabilities

Platform	Sharing of typologies observed by regulated entities.	Adverse incident databases	Messaging communication	Transaction monitoring for alert generation for new risk and patterns based on analytics of combined data	Collaborative intelligence and joint investigations by members with shared access to data	Direct engagement with law enforcement or a dedicated law enforcement unit
Australian Financial Crimes Exchange (AFCX)	Yes	Yes	Yes	No	Partial – isolated examples	Partial
Insurance Fraud Bureau	Yes	Yes	Yes	Yes	Platform-led intelligence function	Broader sector funding of dedicated law enforcement unit
National SIRA – Synectics Solutions	Yes	Yes	Yes	Yes	Yes	No
Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD)	Yes	Yes	Yes	No	Yes	Partial
UK Finance Fraud Intelligence Sharing Service (FISS)	Yes	Yes	Yes	No	Yes	Partial
COSMIC FI-FI Information Sharing Platform	Typologies to be developed and distributed by Monetary Authority of Singapore	Yes	Yes	No	Not currently envisaged	Yes
Money Services Business Industry Negative Database (MSB-IND)	No	Yes	Yes	No	No	No
Transactie Monitoring Nederland (TMNL)	Yes	No	Yes	Partially	No	Partial / Pilot collaboration with Fintell Alliance – a PPP with FIU-NL in an advisory role. There is no direct engagement of law enforcement with TMNL.
314(b) Collaborative Investigation Model	Yes	No	Yes	No	Yes	Yes
Verafin information sharing, operating under USA PATRIOT Act 314(b)	Yes	No	Yes	Partially	Yes	Possible, but not frequent
Salv - AML Bridge	No	No	Yes	No	Yes	Partial (Involvement of FIU)
The Duality AML Information Sharing Network in partnership with Oracle	No	No	Yes	No	No	No
Vocalink - Mastercard Trace and Prevent	Yes	Yes	Yes	Yes	Platform-led intelligence function	No
UK Tri-bank initiative	Partial - New typologies identified through network analysis	No	No	Yes	No	No
Swiss AML Utility	Partial - New typologies identified through network analysis	No	No	Yes	No	No

3.5. Outcomes and impact

As described above, private-private financial information-sharing platforms have widely differing capabilities and processes.

However, at a high level, private-private financial information sharing platforms typically have the following objectives:

- Improved detection of economic crime risk
- Reduction in duplication of processes and cost for pooled activity
- Reduction in risk displacement (for members)

It is also possible that private-private financial information-sharing partnerships can support enhanced resolution on risk which can explain activity which may otherwise be deemed suspicious. This greater resolution on risk can reduce the propensity for financial institutions to deem a client as 'suspicious' and therefore reduce false-positive filing.

In particular, fraud domain platforms have generally been better able to attribute impact in terms of cost savings (from loss to fraud prevented) compared to AML platforms. AML performance indicators remain a challenging area.

Platform	Key outcome metrics
National SIRA – Synectics Solutions	Between May 2020 to May 2021, £1.4bn of fraud loss in the UK is identified as prevented by Synectics Solutions due to National SIRA and associated member collaboration and £5.9bn of loss to fraud is estimated to have been prevented in the five-year period prior to May 2021.
Cifas - National Fraud Database (NFD)	In 2019 just under 365,000 cases were recorded to the NFD. The key outcome metric for Cifas is fraud losses prevented through use of Cifas, which is reported to Cifas by its members through an agreed and structured report. These reports indicate that, during the year of 2019, Cifas members recorded savings of over £1.5 billion in prevented fraud loss.
Transactie Monitoring Nederland (TMNL)	Outcome metrics are still in development. However, an early pilot collaboration between TMNL and the Dutch Financial Intelligence Unit public-private partnership (i.e. the Fintell Alliance) has indicated that substantial efficiency and effectiveness gains can be achieved when mapping out networks of money laundering across multiple financial institutions. In one isolated operational pilot exercise, for example, the time-period for mapping out a complex network was reduced from approximately three weeks to two days (an 85% efficiency gain).
314(b) Collaborative Investigation Model	Since 2015, this model has been applied by major financial institutions in the U.S. to identify thousands of new subjects of interest to law enforcement and contribute to significant charges, convictions, sentences, and asset seizures and forfeitures. On average, for every subject of interest shared by law enforcement agencies through this model, five additional subjects of interest (previously unknown to law enforcement) are identified. Members also report that this model of information sharing has helped them individually to better understand and individually mitigate financial crime risk within their institution.
Verafin information sharing, operating under USA PATRIOT Act 314(b)	Outcome metrics focus on speed and breadth of information sharing under 314(b) Verafin has supported 67,000 collaborations between financial institutions. 55% of responses occur in less than 24 hours; 84% of responses occur in less than 1 week; with the longest collaboration thread being 40 Messages; and 16 institutions participating in one collaboration.

Vocalink - Mastercard Trace and Prevent	Within a few weeks of going live, the following results were recorded: • Thousands of UK accounts were subjected to further investigation due to suspicious activity — a notable percentage of which were subsequently identified as mules. • Multiple, large, well-concealed money laundering rings were uncovered — where money was being moved between networks of accounts and institutions. • Hundreds of mule accounts previously unknown to authorities were identified. Overall the initiative has observed improved detection rates; faster speed of response; reducing consumer impact and dissuading criminals from targeting the participating institution; greater prevention and recovery of funds exiting both the banking system and each participating institution; and fewer attempts at using participating institutions' accounts to extract funds.

Many platforms are only recently developed and therefore it is premature to consider operational or criminal justice outcomes associated to the platform. However, a number of platforms cite learnings and various stages of proofs of concept as significant developments in the global field of private-private financial information sharing to detect and disrupt economic crime. These include:

Platform	Insights, learning and stages of development achieved
314(b) Collaborative Investigation Model	Through developing this model, members have established legal and governance framework for financial institutions to engage in data sharing, network analysis and joint investigations as authorised by 314(b).
Transactie Monitoring Nederland (TMNL)	As an operational model has expanded its proof-of-concept value to establish an analytics roadmap, focused primarily on simpler rule-based models already proven in the proof of concept. Together with banks, TMNL demonstrated that the end-to-end process - from data-collection, to alert generation, and finally alert review - can operate effectively. Alerts have been delivered in a consistent two weekly cadence. TMNL has delivered alert generation that banks cannot generate individually, based on the respective data scope (business clients). TMNL also report qualitative benefits from interaction within TMNL, including: i) knowledge sharing; ii) efficient throughput times both on model development and multibank investigation; iii) collective investment to gain deep insights relevant to large investigations.
Salv - AML Bridge	Ahead of the initial six-month pilot, AML Bridge reported achievements in setting up the governance model, conducting legal analysis and selecting relevant use cases, building the technology, setting up the contractual framework, and identifying appropriate privacy protecting technology framework, with engagement from the data protection supervisor. Operational since July 2021, Salv reported in February 2022 that the AML Bridge generated 750+ collaborative investigations. 75% of collaborative investigations on cases marked urgent were initiated within one hour and 90% within two and a half hours, with a median first response time of 18 minutes.
Vocalink - Mastercard Trace and Prevent	At the proof-of-concept stage, two years of Faster Payments transaction data was brought together, connecting nearly 100 million accounts across financial institutions and detailing over 357 million transaction relationships. The proof of concept identified money mules' behaviour in respective financial institution and different targeting techniques, extraction techniques, the speed of movement. The model proved that money mule networks could be visualised across multiple financial institutions, that money mules were revealed which had not been otherwise detected through a financial institution normal control framework, and that proceeds of crime through money mule networks were able to be mapped and traced across multiple financial institutions.

UK Tri-bank initiative	UK Tri-bank report success in achieving the objectives of the pilot which were to: - Encrypt and extract transaction data from participant institutions in a manner that protects personally identifiable information within the original data; - Build a network of the encrypted data in order to build a view of the payment behaviour; - Inject known Financial Crime typologies into the network and apply a data led approach to identifying unusual behaviour; and - Identify potential instances of criminality that would not have been identifiable without aggregating data.
Swiss AML Utility	Legal opinion secured and presented to the Swiss financial regulator; production architecture is envisioned, federated learning model established, data access control to receive and contribute data based on bank's risk appetite and strategy is achieved.

However, many of the platforms surveyed in this study have raised challenges in measuring performance in terms of the impact on financial crime.

Both in fraud and AML domains, performance metrics can be difficult for a central platform to monitor. Platforms can describe outputs and the number of investigations taking place through the platform. However, with the notable exception of the Singapore COSMIC proposals, platforms do not generally have visibility over the determination and final decision making that a member has taken with regard to a case.

In terms of end-to-end effectiveness, a number of platform owners described the lack of visibility of law enforcement action on the identified criminality and the sense that the initiatives were engaged in a continual 'whack-a-mole' without truly disrupting the underlying organised crime activity.

Lack of public sector responses to intelligence produced by the private sector was a common feature in challenges described by both fraud and AML domain platform owners.

3.6. How much data is involved?

Platforms have demonstrated that large amounts of data can be processed securely and efficiently. The volumes of data shared, and whether the platform itself has direct access to the data, varies according to the different platforms, as follows:

Platform	Scale of data involved and membership
Australian Financial Crimes Exchange (AFCX)	In early 2022, AFCX had 16 members and had processed approximately 19 million cases, with approximately 480 million data elements. The database of adverse incidents was assessed to be growing at approximately 100,000 records per week.
[United Kingdom] National SIRA – Synectics Solutions	As at 1 June 2021, Synectics has over direct 120 clients with licenses for use of National SIRA or SIRA enterprise, across finance; insurance; telecommunications; and vehicle rental sectors. There are over 20k fields available within the SIRA schema and, as at June 2021, National SIRA had over 1.2bn rows of data loaded by clients in the previous 12 months.
[United Kingdom] National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) – Cifas	In June 2021, there were just under 600 organisations in Cifas membership (a full list of those members can be found on the public Cifas website). National Fraud Database (NFD) is the UK's largest repository of fraud risk information: information that can be used by Cifas members to reduce exposure to fraud and financial crime and inform decisions according to your organisation's risk appetite. Enhanced Internal Fraud Database (EIFD holds fraud risk data relating to internal fraud threats, such as bribery and corruption, theft of personal and/or commercial data, customer account fraud and false applications (including fake qualifications). The 'Fraudscape report'[39] highlights that 2021 saw over 360,000 cases of fraudulent conduct recorded to the NFD. Identity fraud accounts for 63% of all cases and the number of cases recorded has grown by 22% (226,000) in 2021.
[United Kingdom] Vocalink - Mastercard] Mastercard Trace and Prevent	Proof of concept connected two years' worth of Faster Payments transaction data in order to build a model of the UK's payments network, connecting nearly 100 million accounts across 12 financial institutions and detailing over 357 million individual payment relationships.
[United Kingdom] UK Finance Fraud Intelligence Sharing Service (FISS)	FISS receives 16,000 records, submitted by members, per month.
[United Kingdom] Insurance Fraud Bureau	IFB holds in the region of 145 millions records of claims and policies.
[United States] Verafin information sharing, operating under USA PATRIOT Act 314(b)	Approx 2500 financial institutions using Verafin and over 67,000 collaborations recorded through the platform in 2022.
[Estonia] AML Bridge Salv	As of December 2021, almost the entire Estonian retail banking market (9 retail banks) are connected via the AML Bridge network. The volume of customer data exchanged is controlled by set/closed fields to ensure that only data which is necessary and proportional is sent between network members. This includes customer details such as name, date of birth, source of wealth/funds information, relevant transaction history. Over 750 collaborative investigations have been initiated between July 2021 and February 2022.
[Netherlands] Transactie Monitoring Nederland (TMNL)	Proposal is to support transaction monitoring and alert generation across the five largest financial institutions in the Netherlands. In 2019, the total client portfolio at these financial institutions accounted for 12 billion transactions, across 32 million customers, resulting in over 212 thousand alerts per year. The current scope of TMNL only includes business clients and their transactions.
[United Kingdom] UK Tri-bank initiative - Deloitte UK / FutureFlow - Proof of concept (2018-2020)	3 UK banks, intermediated by Deloitte UK, focused on small and medium sized corporate client data. Within the dataset provided, 200,000 accounts with 45 million payments, that had a common link within the network were identified and analysed.

3.7. What type of data is involved?

Platforms described in this study have widely different sources of input data, as set out below.

UK platforms	
Platform	**Nature of input data**
UK Tri-bank initiative	- SME Corporate client transaction data.
Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD)	- Fraudulent events as submitted by members, including: o Identity Fraud – When a Subject abuses personal data to impersonate an innocent party, or creates a fictitious identity, to open a new account or Product. o Facility takeover – When a Subject abuses personal data to hijack an existing Product. o False Application – When an application for a product is made with material false-hoods. o Asset conversion – The unlawful sale of an asset subject to a credit agreement. o Misuse of facility – The misuse of a Product. o False insurance claims – When an insurance claim or supporting documentation of a claim contains a material falsehood. See the CIFAS Fraudscape report for details on the breakdown of data reported to CIFAS.[40] - And third-party data sets shared to members o Fraudulently Obtained Genuine documents (FOG); o 'Amberhill' data (false identity documents obtained from ID factory raids); o Law enforcement alerts; o General Register Office deaths data.
National SIRA – Synectics Solutions	- Member reported adverse data points associated to an individual, access to closed data syndicate and additional database.
UK Finance Fraud Intelligence Sharing Service (FISS)	- Payments fraudulent events as submitted by members.
Insurance Fraud Bureau	- Insurance policy and claim data, adverse data and investigations and messaging.
Vocalink - Mastercard Trace and Prevent	- All relevant payments data.

Non-UK platforms	
Platform	**Nature of input data**
COSMIC FI-FI Information Sharing Platform	- Queries and alerts related to AML investigative information and client exits.
Salv - AML Bridge	- Relevant and necessary customer and transaction data for AML, fraud and sanctions investigation queries.
Swiss AML Utility	- Corporate data AML Alerted entities.

Transactie Monitoring Nederland (TMNL)	- Business client's transaction data.
Money Services Business Industry Negative Database (MSB-IND)	- Exited MSB agent operator information.
314(b) Collaborative Investigation Model - a formal association of financial institutions registered under USA PATRIOT Act 314(b)	- Information relevant to law enforcement investigations, shared under 314(a) of the USA PATRIOT Act, or members' own information initiates a case investigation. The information is then augmented through this model and enriched through collaborative network analysis. Data from members institutions relevant to an investigative case is pooled and analysed in a common data platform.
The Duality AML Information Sharing Network in partnership with Oracle	- Alert triage and AML investigative queries, as pre-authorised by members, and supported by 314(b).
Verafin information sharing, operating under USA PATRIOT Act 314(b)	- AML investigative queries shared under the authority of 314(b). The platform also includes all transaction data for relevant customers who subscribe to transaction monitoring and automated filing through Verafin.
Australian Financial Crimes Exchange (AFCX)	- Member data relating to confirmed fraud, cybercrime, scams and money mule activity.

Some platforms have access to broad transaction (or insurance policy) data regardless of whether it has been previously alerted for AML purposes. These platforms include Vocalink - Mastercard Trace and Prevent, UK Tri-bank initiative, National SIRA – Synectics Solutions and the UK Insurance Fraud Bureau.

However, the majority of private-private platforms must operate from data which is less broad and has some level of threshold to it or is based on information that is 'alerted' by a member.

Platforms that revolve around adverse incident databases typically rely on their members use of the identified high-risk entities in the database to discover additional entities of concern and, if appropriate, file any newly discovered risk accounts to the database. This is the case for Money Services Business Industry Negative Database (MSB-IND), the COSMIC FI-FI Information Sharing Platform, the Australian Financial Crimes Exchange (AFCX), Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) and the UK Finance Fraud Intelligence Sharing Service (FISS).

The Singapore COSMIC FI-FI Information Sharing Platform straddles a number of capabilities based on queries and alerted information sharing. At a level of initial assessment of suspicion, COSMIC is a messaging platform (REQUEST functionality). At higher thresholds of concern, COSMIC enables proactive notifications to counterparties about the risk discovered by an initial financial institution's investigation (the PROVIDE functionality). At a level of suspicion and client exists, COSMIC provides an adverse incident database capability (the ALERT functionality). While member financial institutions are not envisaged to directly engage with a central analytical capability, the Monetary Authority of Singapore will have the authority to run network wide analytics over this body of data (which is still based on an initial threshold of concern and is not full transaction monitoring).

A key variable then for platforms is what threshold of input data they use. This has wide ranging implications for the capabilities of the platform and the interaction with data protection considerations.

The use of privacy preserving technology can allow for reduced disclosure of input data, somewhat changing the dynamic as to whether large amounts of input data necessarily entail a large amount of disclosure or 'sharing' of information.

	Platforms that make use of wide transactional input data	Platforms that work only from 'alerted' data from members
Non-UK platforms	- Transactie Monitoring Nederland (TMNL) - The Duality AML Information Sharing Network in partnership with Oracle	- COSMIC FI-FI Information Sharing Platform - Salv - AML Bridge - Swiss AML Utility - Money Services Business Industry Negative Database (MSB-IND) - 314(b) Collaborative Investigation Model - Verafin information sharing, operating under USA PATRIOT Act 314(b) - Australian Financial Crimes Exchange (AFCX)
UK platforms	- National SIRA – Synectics Solutions - Insurance Fraud Bureau - Vocalink - Mastercard Trace and Prevent - Tribank	- Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) - UK Finance Fraud Intelligence Sharing Service (FISS)

Network wide transaction or policy data provides a large analytical advantage in discovering previously unknown accounts linked to high-risk or suspicious activity.

Platforms like National SIRA – Synectics Solutions, the Insurance Fraud Bureau and Vocalink - Mastercard Trace and Prevent will send proactive alerts to members when the central analytical capability has identified risk exposure to a criminal network.

Messaging platforms - such as the Salv 'AML Bridge' and The Duality AML Information Sharing Network in partnership with Oracle - where there is no central analytical capability, are not able to proactively alert members to identified risk.

For platforms with limits and thresholds on the input data, there is a benefit in achieving data minimisation and a lower intrusion into privacy, however there is a trade-off in terms of a lower efficacy in being able to identify network wide risks that are not visible to individual members.

For example, sharing on COSMIC is focused on priority risk areas identified in Singapore's National ML/TF Risk Assessment, and a case must cross material risk thresholds before sharing takes place. This could make it more challenging for COSMIC's participating financial institutions to discover 'unknown unknown' threats and typologies – as the platform is relatively more focused on 'known unknowns'. However, it is intended that MAS will complement COSMIC with its own broader AML/CFT surveillance and analysis to identify and alert the private sector to such systemic threats.

This stands in contrast to the approach of the Netherlands' Transaction Monitoring NL (TMNL) which effectively allows for a pooling of minimised transaction monitoring data from participating FIs. The multibank data coverage will allow for a greater efficacy of network analytics to detect criminal behaviour and patterns.

In the Netherlands, since 2019, TMNL has been developed as a platform for a utility-based approach to transaction monitoring. TMNL's objective is to enhance identification of money laundering and terrorist financing through more effective detection of patterns and behaviour on a combined transaction datasets and apply typologies and algorithms to the combined data.

3.8. How are public agencies directly engaged in the platform analysis or start of investigations?

Another difference between platforms surveyed in this study is the extent to which the platforms engage directly with law enforcement agencies, either at the initial stages of case generation or in the submission of the intelligence package to an engaged law enforcement partner.

For some platforms, the engagement of law enforcement agencies is essential and central to the design of the model. The majority, however, only have ad-hoc engagement with law enforcement or one-way flows of information to law enforcement. In this section, we are exploring examples which go beyond the traditional reporting from regulated entities to national Financial Intelligence Units, but highlight platforms that can demonstrate a funded, interested and engage enforcement partner or set of enforcement partners to work from the financial intelligence produced by the platforms.

While the majority of platforms surveyed are private sector or not-for-profit organisations, the Singapore COSMIC Information Sharing Platform is grounded as public sector-led and managed initiatives – though one which has been co-created between the public and private sector. In the case of Singapore, MAS will own and operate COSMIC, and integrate COSMIC data into its own supervisory surveillance. In addition, the Suspicious Transaction Reporting Office, Singapore's FIU, will have access to COSMIC information for its own analytics.

The U.S. 314(b) Collaborative Investigation Model frequently builds on investigative start points provided by public law enforcement agencies. This has made it more likely that the output of an investigation is actionable by authorities and can lead to more timely and effective results.

However, the Singapore COSMIC Information Sharing Platform and the U.S. 314(b) Collaborative Investigation Model are the only platforms surveyed in this study where the involvement of law enforcement or public agencies is central for their normal operations. Even in the case the U.S. 314(b) Collaborative Investigation Model, the role for public agencies is not essential and not always part of an investigative process. Both of these partnerships are in the AML domain and no platforms that are exclusively in the fraud domain have a similar involvement of public agencies. No UK ECR private-private platforms benefit from public agencies directly engaged in the platform analysis or start of investigations

Platform	Relationship with law enforcement
COSMIC FI-FI Information Sharing Platform	Within the current proposal, MAS will own and operate COSMIC and integrate COSMIC data into its own supervisory surveillance. The Suspicious Transaction Reporting Office, Singapore's FIU, will have access to COSMIC information for its own analytics purposes.
Insurance Fraud Bureau	Since 2012, the Association of British Insurers has provided funding to a dedicated law enforcement unit (IFED) within the City of London Police. While IFB provides intelligence packages to IFED, IFED is not essential or central to the operations of the IFB.
Australian Financial Crimes Exchange (AFCX)	No essential or central relationship with law enforcement agencies at the operational level. Ad hoc engagement is observed in specific initiatives and public sector representation exists at a Board level.
Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD)	No essential or central relationship with law enforcement agencies. Cifas data has a feed into the National Fraud Intelligence Bureau.
314(b) Collaborative Investigation Model - a formal association of financial institutions registered under USA PATRIOT Act 314(b)	This model relies on strong relationships with law enforcement agencies, which - via 314(a) of the PATRIOT Act and with the support of FinCEN - frequently provide start points to initiate cases. Such law enforcement

	engagement improves the likelihood that the outputs from an investigation are actionable by law enforcement authorities.
The Duality AML Information Sharing Network in partnership with Oracle	No essential or central relationship with law enforcement agencies.
Money Services Business Industry Negative Database (MSB-IND)	No essential or central relationship with law enforcement agencies.
National SIRA – Synectics Solutions	No essential or central relationship with law enforcement agencies. Law enforcement engagement can be limited, with the platform revolving around commercial services to members (who may themselves have direct engagement with law enforcement agencies).
Salv - AML Bridge	Some engagement with the FIU at a process/governance level.
Swiss AML Utility	No essential or central relationship with law enforcement agencies.
Transactie Monitoring Nederland (TMNL)	No essential or central relationship with law enforcement agencies, though the platform has a priority to enhance the engagement and information flow with the FIU and law enforcement perspectives.
UK Finance Fraud Intelligence Sharing Service (FISS)	No essential or central relationship with law enforcement agencies. However, UK FISS data is fed into the National Fraud Intelligence Bureau as a dedicated unit.
UK Tri-bank initiative	No essential or central relationship with law enforcement agencies.
Verafin information sharing, operating under USA PATRIOT Act 314(b)	No essential or central relationship with law enforcement agencies.
Vocalink - Mastercard Trace and Prevent	No essential or central relationship with law enforcement agencies. Law enforcement engagement can be limited, with the platform revolving around commercial services to members (who may themselves have direct engagement with law enforcement agencies).

The Insurance Fraud Bureau has raised the value in their role of 'shepherding' information collection processes that are useful to IFED and other law enforcement and ensuring there are good lines of communication and smooth processes where appropriate.

The Insurance Fraud Bureau have also pursued alternative disruption collaborations to mitigate insurance fraud threats. Where there are regulatory or conduct issues on the part of solicitors associated to a fraud case, the Insurance Fraud Bureau will make referrals to the Solicitors Regulation Authority. As a large proportion of insurance fraud is associated to identity theft, the Insurance Fraud Bureau liaises closely with the Information Commissioner's Office on potential offences that fall within the ICO's mandate.

However, despite this extensive liaison with enforcement and regulatory bodies to achieve disruption, the IFB assesses there to be a gap between the public sector capacity to respond to fraud threats and the extent of those threats. The IFB is looking at alternative methods of disruption including regulatory intervention, civil sanction especially where the standard of evidence may not support a strong case for criminal prosecution.

UK FISS data is fed into the National Fraud Intelligence Bureau as a dedicated unit. With regard to wider forums connected to UK Finance, the Dedicated Card and Payment Crime Unit (DCPCU) is worthy of note. The DCPCU was formed as a partnership between UK Finance, the City of London Police and the Metropolitan Police Service together with the Home Office to target fraud organised crime. Throughout 2020 the unit prevented an estimated £20 million of fraud, arrested 122 suspected fraudsters, and carried out enforcement activity against criminals exploiting Covid-19 to target their victims. The unit has also worked with social media platforms to take down over 700 accounts linked to fraudulent activity in 2020, of which over 250 were money mule recruiters.[41] In addition, UK Finance and UK Finance members take part in the Joint Money Laundering Intelligence Taskforce (JMLIT) as a public-private partnership.[42]

The Insurance Fraud Enforcement Department (IFED)[43].

The IFED was set up in 2012. It is a bespoke unit within the City of London Police dedicated to combatting insurance fraud. IFED is funded by the insurance industry via the Association of British Insurers (ABI) and has a remit to investigate insurance fraud throughout England and Wales.

The unit comprises of four operational teams made up of Detective Constables and Financial Investigators, each managed by a Detective Sergeant. Each team deals with a high number of investigations, using both traditional policing methods as well as proactive and disruptive tactics to fight insurance fraud.

A fifth team, the IFED Hub, consists of a Detective Sergeant, Senior Analyst, and Police Staff, who provide intelligence analysis and research as well as administrative support to the department and industry.

According to the City of London Police website, since its inception, IFED has:

- Arrested and interviewed over 2,700 suspects
- Secured over 1,000 convictions and cautions
- Recovered assets worth almost £3 million

IFED also emphasizes the importance of preventing and deterring fraud through stakeholder engagement and campaigns or one-to-one liaison with industry members.

Most private-private ECR collaboration platforms do not benefit from a strong and direct link with a dedicated law enforcement agency – almost none benefit from either law enforcement inputs on typological intelligence on criminal behaviours or to feed in specific targets to private-private collaborative analytics, and only a minority have links to a dedicated law enforcement unit to respond to the intelligence developed by private-private ECR collaboration.

Multiple platform owners interviewed in this study, particularly in the fraud domain, raised challenges about the lack of public sector engagement in the intelligence produced by the private sector or the limited bandwidth of the public sector to take up cases – even in cases where a dedicated law enforcement unit is linked to the ECR platform.

3.9. Is the data centralised or decentralised?

The majority of private-private financial information-sharing platforms rely on centralised pooling of relevant data.

However, two platforms surveyed, predominantly AML domain platforms, rely on privacy preserving techniques[44] to be able to utilise analytics on the networked data, but without requiring data to be centralised.

- Salv 'AML Bridge' relies on end-to-end encryption facilitating messaging between regulated entities and the platform has no access to the underlying data nor central analytical capability over the data shared.
- Similarly, The Duality AML Information Sharing Network in partnership with Oracle supports peer-to-peer queries without centralising any data, nor revealing the subject of the query itself to the requested party.

	Is data centralised in the platform	
	No	**Yes**
AML	- Salv - AML Bridge	- COSMIC FI-FI Information Sharing Platform - Transactie Monitoring Nederland (TMNL) - UK Tri-bank initiative - Swiss AML Utility
Both fraud and AML	- The Duality AML Information Sharing Network in partnership with Oracle	- Money Services Business Industry Negative Database (MSB-IND) - 314(b) Collaborative Investigation Model **Data relevant to investigations is pooled on a common platform.* - Verafin information sharing, operating under USA PATRIOT Act 314(b) - Vocalink - Mastercard Trace and Prevent[45] - Australian Financial Crimes Exchange (AFCX)
Fraud		- Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) - National SIRA – Synectics Solutions - UK Finance Fraud Intelligence Sharing Service (FISS) - Insurance Fraud Bureau

The Vocalink 'Mastercard Trace and Prevent' system takes a different tack, in that no additional data is requested from members, but - rather - the existing payments networked data is used to analyse risk. In a sense, this model represents pre-existing pooled data relevant to the clients of multiple financial institutions. However, it does not require additional pooling of data beyond what is normally available to a payments provider.

In some cases, the platform will have no access to underlying raw data, but the transaction data will still be centralised for link analysis.

This is the case for the Swiss AML Utility, Transactie Monitoring Nederland (TMNL) and the UK Tri-bank initiative, which all support network analytics (though the Swiss AML Utility is limited to alerted input data), but the minimised data is still centralised. However, the central analytical capability does not have full access to the underlying data because of one-way hashing or other encryption techniques. Therefore, TMNL does not have access nor visibility of raw personal data.

In Duality's case, privacy preserving analytics allows the requester to send a query without divulging details of the subject of the query to the requested party.

Salv AML Bridge uses end to end encryption to support messaging without having any access to the message content, unlike COSMIC FI-FI Information Sharing Platform or Verafin information sharing, operating under USA PATRIOT Act 314(b), where messaging is visible to the central platform and open to network-wide analytics.

Fraud-dedicated platforms surveyed in this study generally centralise data, often make use of non-alerted data and also share data without the use of advanced privacy enhancing technologies for securing data 'in use'. In these examples, the central analytical hub has access to the raw contributing data and any (authorised) party using or analysing the data has access to the raw data. This does not entail that the data is not held securely, as the platforms will meet encryption standards for data in storage and at rest, but such the platforms do generally have access to the full underlying data, in contrast to privacy preserving platforms.[46]

3.10. Who determines economic crime risk that is communicated to members?

A key distinction to make between the platforms surveyed in this study is the different assigned roles for platforms and members in identifying economic crime risk.

In a number of examples, the purpose of the platform is to discover ECR risk that individual financial institutions (or others) would not be able to identify alone and then alert those members to the risk.

Platforms that take a role in identifying, assessing and alerting on risk (that has not otherwise been identified by members) include: the Swiss AML Utility, the Transactie Monitoring Nederland (TMNL), the UK Tri-bank initiative and Vocalink - Mastercard Trace and Prevent.

Some platforms seek to provide an opportunity for members share individual elements of economic crime risks, that the members themselves have identified, which are shared on a reciprocal basis with other members. Again, this sharing supports awareness across different members of information that would have been difficult or impossible for members to identify in isolation.

A number of platforms do not have a role in identifying tactical economic crime risk (that has not already been identified by at least one member) and, instead, they provide resources for members to receive information, shared by other members.[47] This format is part of the design of the Duality AML Information Sharing Network in partnership with Oracle, Salv - AML Bridge and the Money Services Business Industry Negative Database (MSB-IND).

Models like the Insurance Fraud Bureau supplement member reported adverse incidents with an intelligence and analytical capability at the platform level. The 'IFI Hub' of the Insurance Fraud Bureau combines policy/transactional data, adverse incidents and information receive information from the police, or from the public, or the Insurance Fraud Bureau's own analytics to designate a high-risk network. This can be generated out as a warning to insurers.

In some models, the platform and member investigative capacity are one and the same concept. In the 314(b) Collaborative Investigation Model, investigators from individual member financial institutions can come together to collaborate in real-time on a case. In this example, there is no platform or resources for analysis which is independent and distinct from the membership, but the members second resources and staff to form the centralised analytical resource.

3.11. Does the platform generate intelligence on new typologies of crime?

Where the central platform has access to underlying data, there is the potential to discover and refine typologies of suspicion and support machine-learning techniques to discover associations in connected data that would not be observable to a human analyst.

The Swiss AML Utility, Transactie Monitoring Nederland (TMNL) and Tri-bank initiative each sought to demonstrate this capability as a core element in their proof-of-concept phase.

Adverse incident databases do not typically have the same data-driven capability to generate network typologies of crime, but can and do support typology development through pooling of knowledge from human analysts and available insights from individual incidents.

UK National SIRA – Synectics Solutions supports members to create and share crime-specific behaviour models and conduct link analysis to identify, monitor and prevent organised fraud networks (within the 'Orion' product). In addition, Synectics apply a machine learning national model and predictive analytics to support members to identify fraud risk. Further analytics at the platform level are available through the serious investigations unit (SIU), which is a platform capability that provides additional analytical resource to members in cases of suspected serious organised crime.

Vocalink apply machine learning techniques which are trained on over 20 billion transactions amounting to trillions of pounds in value to identify risk across the wider payments network. As such, 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.

The Singapore COSMIC Information Sharing Platform takes a different approach in focusing sharing on key risk areas outlined in the National Risk Assessment.[48] Within these key risks, sharing may take place if a case crosses material risk thresholds. Red flags to define those thresholds have been co-developed with the COSMIC participating banks, based on common typologies in these risk areas. Additional risk areas and red flags may be added in future phases of COSMIC, co-developed by members, to expand COSMIC's coverage and adapt to changes in criminal methods.

Due to Verafin's position as a messaging platform provider, but with parallel solutions to support individual members transaction monitoring, Verafin can develop data-driven typologies and distribute them to members and, even, proactively alert members who have exposure to the typology.

The UK Finance supports both the UK Fraud & Financial Crime Alerting Services (FCAS) as a centralised alert portal for members and key partners to "access timely, actionable intelligence products helping to inform strategies, identify victims and prevent and detect economic crime"[49] and also a range of intelligence forums which allow members to share insight and key intelligence. UK Finance Threat working groups are also responsible for developing industry workplans to combat threats in their subject matter areas. UK Finance has a central intelligence unit responsible to support this process and for the operations of the FISS system. Intelligence shared through FISS informs the work of the UK Finance intelligence unit in analysing the current financial fraud landscape. UK Finance and its members will also engage with the UK JMLIT to support the development of typological and strategic intelligence products, which may be distributed to members through FCAS.[50]

3.12. What legislative basis enables the information-sharing through platforms?

The legislative basis for private-private financial information-sharing varies considerably between countries and domains.

In Australia, the privacy statute permits the collection, use and sharing of personal information with consent or where an entity suspects that unlawful activity, or misconduct of a serious nature has been, is being or may be engaged in and the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.

In the UK, information-sharing for the purposes of fraud prevention benefits to some extent from enabling legislation through the Serious Crime Act 2007 and UK fraud domain platforms are typically designated as a Specified Anti-Fraud Organisation (SAFO) by the UK Home Office under the same legislation. However, this SAFO designation supports only public sector sharing of data with a SAFO. It is not a legislative vehicle for private-to-private data sharing or place any requirement on public bodies to share fraud data with a SAFO. In general, in the UK, there is no specific enabling legislation to support economic crime-related information-sharing in the UK. Fraud platforms, of which there are a number in the UK, generally make use of a 'legitimate interest' basis under GDPR and Recital 47 of GDPR.[51]

In terms of AML platforms in the UK, the UK tri-bank initiative focused on processing corporate transaction data, which was outside the scope of GDPR. However, it should be noted that some business client data would be considered personal data – for example single proprietor legal entities or companies with limited number of beneficial owners. In contrast, the U.S. and Estonia both benefit from a specific legal basis to enable private-private sharing for AML purposes. In addition, to facilitate the COSMIC model, Singapore has proposed legislative changes and is consulting on those requirements.

In Estonia, the AML law permits private-private sharing only in cases of alerted or high-risk customers or in relation to suspicious transactions. It is possible (or arguable) that 314(b) of the U.S. PATRIOT Act may be used to support information sharing at a lower threshold of concern – potentially enabling transaction monitoring utility-style network analytics – however, during this research process, it was explained by interviewees that general and historic use of 314(b) relies on an alert as a threshold for information-sharing.

As with the UK tri-bank initiative, Transactie Monitoring Nederland (TMNL) operates on business clients' data. While UK tri-bank initiative operates outside the scope of GDPR, TMNL operates within the scope of GDPR due to the fact that a limited amount of personal data associated to companies is being processed by TMNL. However, the Dutch government is progressing with legislative reform to support private-private AML/CFT information sharing and extend information sharing of personal data. [52]

In the absence of a clear legal basis to support, permit (and, in some cases, require) the information sharing, there can be countervailing legal risks which inhibit the information sharing. Several platforms highlighted the following legal risks which – without a clearer policy position – inhibit the engagement from financial institutions in information-sharing exercises:

- Data privacy risk;
- Civil damages;
- Defamation;
- Competition law risk; and
- AML framework prohibitions around 'tipping off'.

	No specific ECR enabling legislation (enabled through privacy law exemptions)	Specific ECR enabling legislation
Non-UK platforms	- Swiss AML Utility - Transactie Monitoring Nederland (TMNL) [53] - Australian Financial Crimes Exchange (AFCX)	- Salv - AML Bridge - Money Services Business Industry Negative Database (MSB-IND) - 314(b) Collaborative Investigation Model - The Duality AML Information Sharing Network in partnership with Oracle - Verafin information sharing, operating under USA PATRIOT Act 314(b) - COSMIC FI-FI Information Sharing Platform ***(Proposed specific enabling legislation)***
UK platforms	- UK Tri-bank initiative - Vocalink - Mastercard Trace and Prevent - Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) - National SIRA – Synectics Solutions - UK Finance Fraud Intelligence Sharing Service (FISS) - Insurance Fraud Bureau	

Note: *While GDPR can be viewed as an enabling piece of legislation for (at least) fraud prevention information sharing by virtue of the 'legitimate interest' basis and recital 47 – and due to the fact that a large number of fraud prevention platforms surveyed in this study rely on GDPR as the basis for the information sharing – in this section we are primarily concerned with whether a piece of legislation actively authorises the information sharing to take place and that legislation is designed for an ECR purpose.*

3.13. The relationship between information-sharing platforms and privacy statues

All private-private ECR information sharing platforms surveyed are designed to operate within the boundaries of relevant privacy statutes.

However, it is generally the case that fraud and AML information sharing are treated differently under respective privacy regimes. In a number of jurisdictions, privacy laws have exemptions for information-sharing for the purpose of fraud prevention, whereas it is less common that a jurisdiction's privacy laws include an explicit exemption for AML information sharing.

A key privacy statue of relevance to this study is the EU General Data Protection Regulation (GDPR). A number of the platforms surveyed in this study operate within a GDPR jurisdiction and, if other platforms involve EU citizen's data, extra-territorial application of GDPR may also be a relevant factor for the platform's design.

Within the GDPR framework, Recital 47 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."[54]

As the examples of CIFAS and National SIRA set out below, UK fraud domain platforms typically rely on a public interest justification for information sharing, combined with a clear legal basis for information sharing.

The UK Cifas National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) and GDPR

The UK Cifas National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) relies upon Article 6(1)(f) GDPR ("legitimate interests") as the lawful basis for processing.

As the processing involves the alleged commission of offences by the data subject, Cifas relies upon paragraph 14 of Schedule 1, Part 2 of the Data Protection Act 2018 ("preventing fraud") as the substantial public interest condition required by sections 10 and 11 of the DPA2018.

Cifas is a specified anti-fraud organisation under the terms of section 68 Serious Crime Act 2007, which provides public authorities with the legal power to share information with Cifas for fraud prevention. Cifas is certified to ISO/IEC 27001:2013, the international standard for operating an information security management system, and to Cyber Essentials, the online security scheme run by the Government's National Cyber Security Centre.

In terms of purpose limitation, the Cifas system is used solely by members to prevent, detect and disrupt fraud and wider economic crime. To use the database, a Cifas member must operate within the terms of the National Fraud Database Handbook – a guide that sets out eight Principles of use with accompanying guidance. These Principles and guidance describe the controls in place to protect the data on the database, and ensure fairness and transparency.

It is a condition of being a specified anti-fraud organisation that the Information Commissioner's Office be given access to audit and inspect data sharing arrangements between public authorities and Cifas; the ICO audited Cifas in 2014.

The GDPR lawful basis for Cifas information-sharing through the National Fraud Database is legitimate interest, drawing on the General Data Protection Regulation gives fraud prevention as an example of a legitimate interest (Recital 47).

Any business sharing data would need to ensure that information is shared in line with the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation. A vital part of any private-to-private information sharing would be to ensure that data controllers include appropriate safeguards and mitigations in place to address any data protection risks or concerns, which should be set out in their data protection impact assessments (DPIAs). The Information Commissioner's Office would continue to regulate the data protection legislation.

UK National SIRA – Synectics Solutions and GDPR

UK National SIRA operates under UK Data Protection Act 2018, within the GDPR framework. Sharing takes place pursuant to a National SIRA membership agreement which is governed by the National SIRA Operating Rules. For GDPR purposes, Synectics is a joint data controller for National SIRA and Synectics actively manages compliance with GDPR and the Data Protection Act 2018. Data is processed by Synectics under the lawful basis of "legitimate interest" for the purposes of (limited to) the prevention and detection of fraud. The purpose of processing also includes testing and development of the National SIRA Service. Regular audits take place on members to ensure data protection compliance.

National SIRA decisions may be made by automated means, such that members may automatically determine risk if:

- processing reveals behaviour to be consistent with that of known fraudsters or money launderers; or is inconsistent with previous submissions; or
- subjects appear to have deliberately hidden their true identity.

Subjects maintain all relevant GDPR rights in relation to automated decision making.

In addition, Synectics Solutions is designated as a SAFO by the UK Home Office under the Serious Crime Act 2007 and meets ISO 27001 standards for information sharing.

It should be noted that both AML and fraud domain information-sharing platforms are in operation within GDPR jurisdictions and GDPR does not exclude the opportunity for ECR private-private information-sharing.

In terms of the AML domain, there is currently substantial legal analysis underway in the UK, involving the UK government and industry stakeholders, to consider whether AML-domain information-sharing may likewise be justified under a GDPR lawful basis of 'legitimate interest'.

Keeping within GDPR jurisdictions, another route taken by private-private financial information sharing platforms is to limit data processing to sources which are not subject to GDPR requirements or other privacy law statutes. This is the case for Tri-bank information-sharing data, which focuses on business clients' data for example.

Despite the UK examination of the limits of 'legitimate interest' with respect to AML information sharing, current AML platforms surveyed in this study generally rely on a clear enabling law, rather than an exemption to the respective private statute. This is the case in Estonia and the U.S. for example, where a clear and bespoke legislative regime supports the information-sharing.

3.14. What purpose limitations are set in place by different platforms?

The 'UK Economic Crime Plan 2019-2022'[29] highlighted the importance of a more joined-up approach to tackling both fraud and money laundering, under a broader plan for tackling 'economic crime'.

However, in contrast to this broader view on economic crime, UK platforms tend to be restricted in purpose to one domain. UK private-private financial information sharing platforms are mostly made up of fraud domain platforms. UK fraud platforms, in practice, are limited in engaging in anti-money laundering information-sharing because of the clearer basis (and established consensus behind) fraud prevention as a public interest basis for information sharing under data protection law. As a similar consensus has not been established for sharing of AML concerns, these platforms appear - de facto - to be restricted to fraud-prevention domain information sharing.

With regard to UK Cifas, under the current legal framework, Cifas is permitted to share fraud data and has established GDPR compliant processes. The Cifas articles of association include provisions for the prevention of money laundering, in addition to fraud. Members can therefore also use the fraud risk data shared through Cifas to help prevent and detect money laundering. However, money laundering and terrorist financing information is not currently shared through Cifas.

The 'Vocalink - Mastercard Trace and Prevent' use-case covered in this report is for money mule identification and is a fraud prevention domain platform. It is not clear whether other forms of fraud or AML issues will be (or could be) covered by this platform under the current legal framework.

Outside of UK platforms surveyed in this study, no other platforms are limited to fraud prevention by their statute. In addition, outside of the UK, a number of platforms are authorised for information-sharing specifically through AML/CFT legislation and for AML/CFT purposes but may also engage in fraud prevention activities.

The U.S. Section 314(b) of the USA PATRIOT Act authorises information-sharing for the purpose of better identifying and reporting potential money laundering or terrorist activities, however fraud information sharing does also take place through 314(b) and this use of 314(b) has been further strengthened by FinCEN in guidance released in 2020. As such, in the U.S., despite the legal framework for private-private information sharing being delineated on AML/CFT matters, there is now established practice and public sector guidance to support fraud-domain information sharing to take place under the same legislative basis. Indeed, a wide range of predicate criminality is within scope of the 2020 FinCEN updated guidance on the use of 314(b).[55]

On 10 December 2020, FinCEN provided a clarification stating that financial institutions "can now share information in reliance on the Section 314(b) safe harbor relating to activities it suspects may involve money laundering or terrorist activity, even if the financial institution or association cannot identify specific proceeds of a Specified Unlawful Activity being laundered. Prior to this clarification, Section 314(b) permitted financial institutions to share information only in situations of suspected terrorism and money laundering."[56]

Further, the updated guidance from FinCEN makes clear that FinCEN's view is that financial institutions may share information about activities as described, even if the activities do not constitute a "transaction" such as an attempted transaction, or an attempt to induce others to engage in such a transaction. This allows financial institutions to avail themselves of Section 314(b) information sharing to address incidents of fraud, cybercrime, and other predicate offenses, where appropriate.[57]

Understanding 314(b) scope of use

For example, the USA Patriot Act Section 314(b) provides a legal basis for financial institutions to share information with one another, under a safe harbor that offers protections from liability, to better identify and report activities that may involve money laundering or terrorist activities. However, for the first 19 years of the legislative gateway's existence there was uncertainty as to whether fraud and cyber threats could be processed through 314(b) requests.

In a landmark speech in December 2020,[30] FinCEN Director described the contribution of 314(b) private-private sharing as "critical to identifying, reporting, and preventing crime. It is an important part of how we protect our national security." Alongside the speech, FinCEN published a new 314(b) Fact Sheet[31] which clarified that[32]:

> *"Financial institutions do not need to have specific information that these activities directly relate to proceeds of an [Specified Unlawful Activity] SUA, or to have identified specific proceeds of an SUA being laundered… Financial institutions do not need to have made a conclusive determination that the activity is suspicious."*
>
> *"Financial institutions may share information about activities as described, even if such activities do not constitute a "transaction." This includes, for example, an attempted transaction, or an attempt to induce others to engage in a transaction. This clarification is significant and addresses some uncertainty with sharing incidents involving possible fraud, cybercrime, and other predicate offenses when financial institutions suspect those offenses may involve terrorist acts or money laundering activities."*
>
> *"In addition, the guidance notes that there is no limitation under Section 314(b) on the sharing of personally identifiable information, or the type or medium of information that can be shared (to include sharing information verbally)."*

This guidance aimed to soften interpretations of 314(b) which limited its use due to an excessive focus on money laundering, to the detriment of being able to process other instances of economic crime risk – including where financial institutions do not have specific information that activities directly relate to proceeds of crime. However, the guidance does not have a force of law and therefore the original lack of breadth in the legislation may still undermine information-sharing due to uncertainties that need to be tested in the courts.

Some platforms have a legal basis in AML/CFT legislation and may (or may not) also have authority to respond to fraud domain use-cases. The Salv AML Bridge and Singapore COSMIC illustrate different approaches.

The Estonian Salv - AML Bridge operates under the authority for information-sharing derived from the national AML/CFT law but has achieved legal clarity that the same law enables Salv members to process fraud/scam cases within the platform. Section 16.1 of the Estonian AML Act provides a broad scope for investigating predicate or associated crimes, pertaining to money laundering and, during the development of Salv AML Bridge, Salv consulted with the Estonian Data Protection Inspectorate and Financial Supervisory Authority on this particular topic to ensure there was legal and regulatory clarity on the issue.

However, in Singapore, the proposed design concept of COSMIC is clear that the tool will be used only for purposes of direct relevance to AML/CFT/CPF investigations. The COSMIC proposal states that "it is intended that such sharing will be permitted only: (a) to address potential ML, TF or PF concerns in key risk areas".[58]

3.15. Liabilities and protections within the process of information-sharing

Again, platforms vary with regard to the protection from civil liability that may be afforded to information-sharing within the platform.

Protections against liability are intended to protect the institutions engaging in information-sharing from claims arising by the subject of the information sharing. Such protections may take the form of protections from liability associated to:

- Data protection
- Competition law
- Civil damages
- Defamation

A principal challenge with regard to protection from liability is the inter-section with data protection principles and any process for customer discovery or appeal/redress process for individual who are wrongly designated as suspicious. This theme is explored later in this study.

The Netherlands 'Joint Action Plan' legislation encompasses – among others - the supporting legal framework for joint transaction monitoring TMNL and exchange of information between the same type of gatekeepers on customers with an increased ML/TF risk and providing clearly defined legal basis for such a mechanism in the context of GDPR data privacy obligations. The Dutch AML Action Plan is accompanied with the publication of additional government research paper reviewing the Dutch legal regime as a whole in the context of the AML Action Plan. The study highlights what is currently possible within the law, what reforms would be required to achieve the ambition of the AML Action plan, and also highlights the design conditions required to be compliant with data protection and competition law.

In Singapore, the Monetary Authority of Singapore intends to confer statutory protection from civil liability to financial institutions which participate in COSMIC. It is intended that these protections will serve to protect the participant financial institutions as follows

> "from undue legal challenges arising from their participation on COSMIC… [and] will provide confidence that legitimate information sharing to highlight higher risk customers and their related activities will not expose them to civil suits, which may be brought about by the very actors that COSMIC seeks to guard against. Such statutory protection is in line with those given to persons filing STRs under the CDSA, which, similar to information sharing on COSMIC, requires disclosure of information where specified threshold conditions are met."[59]

3.16. Is participation voluntary or mandatory?

The Singapore COSMIC proposal refers to aiming to achieve a paradigm shift in information-sharing. To achieve this, Singapore has put in place a number of mandatory requirements and criminal penalties around the policy regime for COSMIC.

COSMIC breaks new ground in AML/CFT private-private information sharing by establishing a penalty for non-response to a COSMIC request and requiring that responses be timely, thereby incentivising rapid responses.

All other platforms covered in this study are essentially voluntary.

3.17. What information-security standards are required by law?

In this section we are not generally referring to the information-security or cyber-security standards of how data is held within the platform itself, but - rather - the information-security standards, commitments and penalties that come with use (and mis-use) of the facility by members or staff within members.

As part of broader governance requirements, some platforms require certain information-security standards around the how information received through the platform is used.

Synectics Solutions – National SIRA requires users to sign a National SIRA membership agreement which is governed by the National SIRA Operating Rules and use of the UK Finance FISS platform and data is governed through relevant data sharing agreements.

A Cifas member must operate within the terms of the National Fraud Database Handbook – a guide that sets out eight Principles of use with accompanying guidance. These Principles and guidance describe the controls in place to protect the data on the database, and ensure fairness and transparency (set out in box below).

Cifas operating principles[60]

A Cifas member must operate within the terms of the National Fraud Database Handbook and 8 operating principles, as follows:

> ***Principle 1: Reciprocity***
> The National Fraud Database relies on member data. Members must contribute their own cases to receive benefit from the data shared by other members.
>
> ***Principle 2: Purpose Limitation (Legitimate reasons for searching)***
> Data from the National Fraud Database can be used in a wide range of situations for the purpose of the prevention, detection and investigation of fraud and financial crime.
>
> ***Principle 3: Transparency***
> Subjects have a right to know how data will be used and how any decisions related to them have been made.
>
> ***Principle 4: Lawfulness***
>
> ***(Searching and filing)***

Subjects must only be searched and filed if they have been legally informed of how their data may be used via a Fair Processing Notice.

(Standard of Proof)
Cases filed to the National Fraud Database must be supported by evidence and meet the 'four pillars' of the Standard of Proof. The Standard of Proof is:

- That there are reasonable grounds to believe that a Fraud or Financial Crime has been committed or attempted;
- That the evidence must be clear, relevant and rigorous such that the member could confidently report the conduct of the Subject to the police;
- The conduct of the Subject must meet the criteria of one of the Case Types;
- In order to file the member must have rejected, withdrawn or terminated a Product on the basis of Fraud unless the member has an obligation to provide the Product or the Subject has already received the full benefit of the Product.

All Subjects involved that meet the Standard of Proof, must be filed to the National Fraud Database.

Principle 5: Fairness

(Proportionality)
Members must ensure that the data is interpreted in a proportional manner according to their own risk appetite and the product being assessed.

(Protecting innocent parties)
Innocent parties should be filed to the National Fraud Database for their own protection and be clearly distinguished from any other Subject involved in the Case.

Principle 6: Accuracy
All data that is captured must be accurate.

Principle 7: Integrity (Security of the National Fraud Database)
Access to the National Fraud Database is restricted and all members must have adequate policies, procedures and technical measures in place to protect the data.

Principle 8: Data Minimisation
Members must be able to retrieve the evidence to support a case filed to the National Fraud Database but they must not hold data indefinitely. Once it's served its purpose, it must be deleted securely and permanently.

Before joining members are trained to ensure that they understand these requirements, and they must be fully compliant before they can access the system. For example, Cifas will check that Fair Processing Notices have been worded and made available to consumers in compliance with GDPR and the specific requirements of the handbook. Once live, Cifas will audit the member's use of Cifas to ensure ongoing compliance with the handbook.

In general, private sector platforms operate under clear terms of contract, MoUs or data sharing agreements, however, most platforms do not have specific legal duties or criminal sanctions in place to avoid mis-use of the facility, akin to COSMIC in Singapore.

The Singapore COSMIC platform proposal establishes a number of legal duties on participant financial institutions. These include requiring financial institutions to:

> (a) ensure that information disclosed on the platform is accurate and complete and to promptly notify MAS and other relevant participant FIs of any error in the information provided, and to rectify such error as soon as possible;
> (b) ensure that any disclosure made in accordance to the information sharing modes of Request, Provide and Alert is done in a timely manner, and within the prescribed time periods; and
> (c) establish and implement systems and processes to safeguard the information disclosed and received.

Participant financial institutions may be subject to penalties if they fail to comply with the above requirements. The Monetary Authority of Singapore propose that financial institutions may be liable on conviction to a fine not exceeding $1 million and, in the case of a continuing offence, to a further fine of $100,000 for every day or part of a day during which the offence continues after conviction. The proposed penalties are aligned with current penalties under section 27B(2) of the MAS Act for breaches of requirements for prevention of ML and TF.

Singapore's COSMIC will have safeguards (including technical and personnel security features) to ensure that Information sharing will be done in a secure and controlled manner. Financial institution participants of COSMIC will be required to restrict staff access to COSMIC, and any platform information obtained from COSMIC, on a need-to-know basis. This would include only allowing designated staff to access COSMIC, and keeping a register of such staff, with timely and regular reviews of this list.

Financial institutions and their officers will not be permitted to disclose platform information to any other person, except in scenarios as expressly provided for under the legislation. It is proposed that unauthorised disclosure of COSMIC information may result in the financial institution being liable on conviction to a fine not exceeding $250,000. Any individual that failed to secure the financial institution's compliance may also be liable on conviction - (a) if the individual committed the offence wilfully, to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both; or (b) if the individual did not commit the offence wilfully, to a fine not exceeding $125,000. The proposed penalties are aligned with section 47(6) of the Banking Act for breaches of requirements relating to the privacy of customer information.

In the U.S., the legal framework for 314(b) information-sharing states that "Each financial institution or association of financial institutions that engages in the sharing of information pursuant to this section shall maintain adequate procedures to protect the security and confidentiality of such information."[61]

While private sector platforms may not have specific statutory penalties associated to mis-use of the facility, misuse would also be regulated by sanctions associated to breaches of the relevant data protection law. GDPR breaches can reach 4% of global turnover.[62]

3.18. Financial exclusion and data correction

Concerns around financial exclusion are a significant, if not a primary policy concern, in terms of negative or unintended potential consequences of enhanced private-private AML/CFT information-sharing.

While it is the purpose of the AML/CFT regime to deny access to the financial system of 'illicit funds', it is not clear that there is a policy consensus in most countries that citizens should be consistently excluded from financial services on the basis of a financial crime risk assessment and outside of a judicial process.

Operating within this somewhat conflicted policy environment, private-private sharing platforms have adopted a range of different approaches.

Some platforms engage directly with the data subject to inform them of inclusion in the platform, while for others – this is prohibited by law. Only a small minority of platforms provide explicit support to a data subject who is seeking data correction. For most platforms it is unclear how a data subject could effectively challenge the validity of assessments and the accuracy of information held on the platform. The majority of platforms surveyed in this study do not provide subject access process which is designed to surface appeals and make relevant corrections based on that subject access request. In GDPR jurisdictions, this is typically because the platform is a data processor and the decision to release information would be made by the contributing party (data controller).

Perhaps most central to this problem, platforms take different views as to whether the objective of the information-sharing is to financially exclude certain individuals or not.

3.18.1. How are data subjects informed of their inclusion in an ECR information-sharing platform?

Platforms vary in how they engage with the data subjects who are associated to wrong-doing.

While there are typically general clauses in place in customer terms and conditions explaining that a customer's information may be shared by the relevant financial institution in efforts to detect economic crime, in this section we are concerned with whether there is a pro-active or re-active notification to the data subject of an explicit instance of information sharing and the nature of that information sharing.

Some platforms in this study are required to inform the relevant data subject of their inclusion in the relevant platform, whereas other platforms are prohibited from doing so by 'anti-tipping off' legal requirements.

Of particular note, Cifas operates a complaints process that provides all individuals with a way to challenge, and if necessary correct or remove, information that may be recorded about them within the National Fraud Database. The first step is for an individual to exercise their right of access to any personal data held about them on the National Fraud Database by contacting Cifas. An individual can then contact the member that recorded the fraud risk information to challenge it, and if an individual is not satisfied with the response, then Cifas will review the complaint. Given the importance of fraud prevention, should the review by Cifas into the complaint find that the evidence supports the risk record it will be upheld and the record maintained. If, however, the evidence is not found to be compelling, or the decision was incorrect, then a record will be removed from the database. In practice it is rare that Cifas and Cifas members do not have compelling, overriding grounds to carry on processing the personal data concerned. Individuals can also approach the relevant regulator (typically the Financial Services Ombudsman) as well as the Information Commissioner's Office at any stage.

Overview of engagement with the data-subject by the platform

Platform	Extent to which data-subject associated to potential wrong-doing is informed of the processing of their data by the platform
COSMIC FI-FI Information Sharing Platform	**Data subject offered opportunity to explain behaviour in interaction with FI prior to COSMIC ALERT filing** MAS will require that, prior to exiting a customer relationship, a financial institution must provide the customer with adequate opportunity to address its concerns. The financial institution must also document its assessment and the results of these checks with the customer.
Insurance Fraud Bureau	**Data subject is informed** With regard to the UK Insurance Fraud Bureau, any individual who has identifying information uploaded to the insurance fraud register (as a confirmed fraud database) must be informed and notified that they have been placed on the register. Grounds for believing fraud has taken place is the balance of probability (civil standard). Members have to have made a decision on the basis of fraud, i.e. to repudiate a claim, or to void a policy on the basis of believing it to be a fraudulent event. It is deliberately designed to be an overt process and is designed as a preventative tool.
Australian Financial Crimes Exchange (AFCX)	• The data subject is not actively informed about their inclusion in the platform.
Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD)	• The data subject is not actively informed about their inclusion in the platform. • However, data subjects may obtain awareness of their inclusion in the platform through a Data Subject Access Request. • Cifas operates a complaints process that provides all individuals with a way to challenge any data held.
314(b) Collaborative Investigation Model - a formal association of financial institutions registered under USA PATRIOT Act 314(b)	• At the level of member financial institutions, customers are not proactively informed that their data has been shared pursuant to a 314(b) and such notification would be in breach of AML anti-tipping off requirements.
The Duality AML Information Sharing Network in partnership with Oracle	• For this platform, no data is visible to the platform and the platform owners have no knowledge of whether a data subject has been processed through the platform. • At the level of member financial institutions, customers are not proactively informed that their data has been shared in a specific 314(b) query and such notification would be in breach of AML anti-tipping off requirements.
Money Services Business Industry Negative Database (MSB-IND)	**Data subject communicated to prior to inclusion in the platform.** As part of the exit process for an agent by a platform member, the agent would be provided with an appeal process and an opportunity to challenge the information associated to their alleged wrong-doing. Agents (data-subjects) included in the platform would have been afforded this process prior to their inclusion in the platform.

National SIRA – Synectics Solutions	• The data subject is not actively informed about their inclusion in the platform. • However, data subjects may obtain awareness of their inclusion in the platform through a Data Subject Access Request. • Data subjects can then challenge the accuracy of data and inferences of wrong doing associated to the platform/member data.
Salv - AML Bridge	• The data subject is not informed about their inclusion in the platform. • Anti-tipping off provisions may apply. • For this platform, no data is visible to the platform and the platform owners have no knowledge of whether the data subject has been processed through the platform.
Swiss AML Utility	• The data subject is not informed about their inclusion in the platform. • Anti-tipping off provisions may apply. • For this platform, no personal data is visible to the platform analysts (beyond transaction behaviour and anonymised reference data).
Transactie Monitoring Nederland (TMNL)	• The data subject is not informed about their inclusion in the platform. • Anti-tipping off provisions may apply. • For this platform, no personal data is visible to the platform analysts (beyond transaction behaviour and anonymised reference data).
UK Finance Fraud Intelligence Sharing Service (FISS)	• The data subject is not informed about their inclusion in the platform. UK Finance, acting in the role of data processor, does afford individuals the right of access to information held within the platform. The decision to release information would, however, be made by the contributing party (data controller).
UK Tri-bank initiative	• The data subject is not informed about their inclusion in the platform. • Anti-tipping off provisions may apply. • For this platform, no personal data is visible to the platform analysts (beyond transaction behaviour and anonymised reference data).
Verafin information sharing, operating under USA PATRIOT Act 314(b)	• The data subject is not informed about their inclusion in the platform. • Anti-tipping off provisions may apply.
Vocalink - Mastercard Trace and Prevent	• The data subject is not informed about their inclusion in the platform. • Anti-tipping off provisions may apply.

As some platforms have no access to information relating to the data subject; some have access to transactional behaviour, but not traditional identifying information; and some have full access and store personal data – the platforms have very different relationships with the data subjects.

However, even comparable platforms in terms of the visibility of the data subject have different processes with regard to informing the data subject about their inclusion in the platform and then there are further differences as to the process or opportunity for redress and data correction by the data subjects.

3.18.2. How can data subjects engage with platforms to correct data?

The table below compares how platforms interact with data subjects based on the following questions:

A. Is identifying information about the data subject available within the central platform?
B. Can data subjects be subject to action as a result of analysis within or through the platform (by virtue of analysis of their transactional behaviour, for example)?
C. Are data subjects proactively informed of their inclusion in the platform or proactively communicated to about their relevant behaviour prior to filing in the platform?
D. Do data subjects have an opportunity to establish whether their data has been processed by the platform?
E. Do data subjects have an opportunity to challenge the accuracy of information held by the platform?

	Question relevant to engagement with the data subject and data correction				
Platform	**A**	**B**	**C**	**D**	**E**
COSMIC FI-FI Information Sharing Platform	Y	Y	Y	N	Y
Insurance Fraud Bureau (Insurance Fraud Register)	Y	Y	Y	Y	Y
Australian Financial Crimes Exchange (AFCX)	Y	Y	N	Y	Y
Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD)	Y	Y	N	Y	Y
The Duality AML Information Sharing Network in partnership with Oracle	N	Y	N	N	N
Money Services Business Industry Negative Database (MSB-IND)	Y	Y	Y	Y	Y
National SIRA – Synectics Solutions	Y	Y	N	Y	Y
Salv - AML Bridge	N	Y	N	N	N
Swiss AML Utility	N	Y	N	N	N
Transactie Monitoring Nederland (TMNL)	N	Y	N	N	N
UK Finance Fraud Intelligence Sharing Service (FISS)	Y	Y	N	Y	Y
UK Tri-bank initiative	N	Y	N	N	N
314(b) Collaborative Investigation Model	Y	Y	N	N	N
Verafin information sharing, operating under USA PATRIOT Act 314(b)	Y	Y	N	N	N
Vocalink - Mastercard Trace and Prevent	Y	Y	N	Y	N

While all platforms allow for information to be shared which may directly impact the data subject, only a small proportion have in place processes which provide the data subject with information about their inclusion on the platform (either proactively or reactively) or an opportunity to correct inaccurate information held by the platform. However, platforms which are data processors under GDPR will rely on members (data controllers) to respond to subject access requests and relevant data corrections. For example, UK Finance would acknowledge any request from an individual to establish whether personal data has been processed by the platform. After appropriate checks, the request would be communicated to the relevant contributing organisation should information be held within the platform and the member would then determine whether to respond to the individual. The individual would have the right to raise a complaint with the Information Commissioner's Office if they felt that the data controller was unreasonable in their response. Each of the members are required to promptly notify UK Finance (and, if relevant, the other participants) if it becomes aware that any Information contributed by it is inaccurate or the integrity of any information contributed by it is compromised and UK Finance will update or correct the relevant information as appropriate.

3.18.3. How platforms engage with the objective of financial exclusion

Some platforms do take considerable steps to provide greater clarity on the intent of the system as far as financial exclusion and the process for citizens to seek data correction or reinstatement in the financial system (or platform members).

Platform	Extent of clarity with respect of the objective of financial exclusion
COSMIC FI-FI Information Sharing Platform	**Financial exclusion is not an explicit objective, but it is intended that COSMIC participants achieve a shared collective awareness of specific identified threats and, one may reasonably expect that there will be more consistent preventative decisions taken, across the COSMIC participating institutions, against specific suspicious actors.** A major pillar of COSMIC is to prevent a customer (that has had an account closed because of financial crime concerns) from establishing an account with a different financial institution, in a situation where there second financial institution would have no visibility of the financial crime concerns identified by the first financial institution. At the highest level of financial crime concern, participating financial institutions are obliged to file an 'Alert' about exited customers which is then made available to other financial institutions. Recipients of such information should not rely solely on information from COSMIC, but should make their own assessments - based on the information they have and from their engagements with the customer. Where there are sufficient concerns about the customer, the recipient financial institution may choose not to onboard them or to terminate existing services.
Insurance Fraud Bureau	**Service exclusion is not an objective.** The Insurance Fraud Bureau in the UK seeks to ensure that a customers entry into the Insurance Fraud Register (a confirmed fraud database) is an overt process, within which the data subject is informed and notified that they have been placed on the register. It is designed to make insurance providers aware of previous risk and take according steps in terms of pricing for that risk, however there is no intent to deny the customer insurance. There is greater clarity in the provision of insurance services (compared to financial services) that insurance services are a legal requirement and therefore it would not be desirable to prevent an individual from securing insurance. However, insurance premiums are adjusted based on identified risk. By informing the data subject of their inclusion on the Insurance Fraud Register it is intended that this acts as a dissuasive factor for the entity concerned as far as engaging in further insurance fraud.
Australian Financial Crimes Exchange (AFCX)	**Exclusion is a common outcome if not an explicit objective.** While the AFCX supports information sharing in relation to the acts associated to fraud and other unlawful activity - particularly in relation to card payment fraud, scams and other acts - there is no deliberate attempt to exclude certain individuals from the financial system.

Cifas - National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD)	**Exclusion is a common outcome if not an explicit objective.** While the ultimate decision-making process rests with its members, Cifas – through the National Fraud Database (NFD) & Enhanced Internal Fraud Database (EIFD) – allows for risk identified by a member to be shared with other members with the intent of preventing that risk from being onboarded by other members. Cifas supports a data correction process but, the overall effect is that an individual entered onto the NFD or EIFD may experience some degree of exclusion.
The Duality AML Information Sharing Network in partnership with Oracle	**An exit decision may be an outcome of an information-sharing process. The decision to exit a client relationship is determined by members of the network, not by Duality Technologies.** As a messaging platform with no visibility over the data being shared, the platform is neutral as to how members use the information.
Money Services Business Industry Negative Database (MSB-IND)	**Exclusion is an objective.** The purpose of the MSB-IND is to prevent exited MSB agents from registering for member MSBs after being exited for financial crime reasons by a member MSB.
National SIRA – Synectics Solutions	**Exclusion may be an outcome of an information-sharing process. The decision to exit a client relationship is determined by members of National SIRA, not by Synectics.** While the ultimate decision-making process rests with its members, National SIRA allows for members to share risk information that may result in a data subject experiencing some degree of exclusion.
Salv - AML Bridge	**An exit decision may be an outcome of an information-sharing process. The decision to exit a client relationship is determined by members of Salv, not by Salv.** As a messaging platform and data processor with no visibility over the data being shared, Salv has no ultimate control over client exit decisions that network members make based on customer data shared within the platform. However, Salv ensures that members commit in the user contract that decisions taken to exit an individual customers would require a full auditable record of decision making, including information shared through Salv. Such information is intended to be reviewable and contestable if a complaint were to be brought before an ombudsman or equivalent. At the time of this research, there are no automated decision-making processes in Salv and no automated black-listing. Ultimately a human agent of the member firm will assess any client exit decision based on each institution's individual risk appetite.
Swiss AML Utility	**An exit decision may be an outcome of an information-sharing process. The decision to exit a client relationship is determined by members of the utility.**

	As a transaction network analysis platform with no visibility over personal data being shared, the platform is able to identify risk associated to client accounts but is not able to identify the accounts and is neutral as to how members use the information. Further, there is no capacity within the model to allow co-member financial institutions to understand exit decisions by other members.
Transactie Monitoring Nederland (TMNL)	**As a data processor there is no objective or engagement by TMNL on the matter of financial exclusion.** As a transaction network analysis platform with no visibility over personal data being shared, the platform is able to identify risk associated to client accounts but is not able to identify the accounts and is neutral as to how members use the information. Further, there is no capacity within the model to allow member financial institutions to understand exit decisions by other members.
UK Finance Fraud Intelligence Sharing Service (FISS)	**Preventative decisions related to service provision for high-risk customers is a common outcome.** While the ultimate decision-making process rests with its members, FISS allows for members to share risk information that may result in a data subject experiencing some degree of exclusion. However, in common with fraud prevention platforms, the objective is to prevent fraudulent events taking place and to stop fraud attacks on legitimate customer accounts, rather than necessarily to exclude certain individuals from financial services.
UK Tri-bank initiative	**As a data processor there is no objective or engagement by the platform on the matter of financial exclusion.** As a transaction network analysis platform with no visibility over personal data being shared, the platform is able to identify risk associated to client accounts but is not able to identify the accounts and is neutral as to how members use the information. Further, there is no capacity within the model to allow member financial institutions to understand exit decisions by other members.
314(b) Collaborative Investigation Model	**An exit decision may be an outcome of an information-sharing process. The decision to exit a client relationship is determined by individual members, not by the 'platform' or group.** This model is focused on case investigations, rather than informing account exit decisions. However, the model can support better communication with law enforcement entities to avoid account closure decisions when this would be detrimental to law enforcement investigation (using the established processes in the U.S. to request that financial institutions keep open an account of interest to law enforcement).
Verafin information sharing, operating under USA PATRIOT Act 314(b)	**An exit decision may be an outcome of an information-sharing process. The decision to exit a client relationship is determined by members of Verafin, not by Verafin.**

	The platform is neutral as to how members use the information. There is no active role by the platform to push information about exit decisions to other member financial institutions.
Vocalink - Mastercard Trace and Prevent	**An exit decision may be an outcome of an information-sharing process. The decision to exit a client relationship is determined by members of Vocalink, not by Vocalink.** As a transaction network analysis platform, the platform is able to identify risk associated to client accounts, but members are responsible for further action against those accounts. Further, there is no capacity within the model to allow member financial institutions to understand exit decisions by other members.

The outlier amongst the platforms surveyed is the Insurance Fraud Bureau, which has a clear policy position that it is not the objective of the platform to encourage exclusion of particular individuals. There is recognition in this model (or, rather, in the insurance sector more broadly) that being denied insurance services is not compatible with operating in society nor in line with legal requirements to have insurance. Rather, the model is focused on understanding risk and pricing accordingly, given the risk of loss to the insurer.

In other platforms, there is often no explicit clarity as to whether financial exclusion is an objective or not, though the use of the platform appears to encourage more consistent service denial decisions against the same customer.

A number of platforms explicitly seek to support exclusion objectives.

The current situation – i.e. that a wide variety of approaches are observed in response to the same fundamental outcome – is the result of lack of clarity at the policy level and indeed at the level of FATF international standards. This lack of clarity on whether consistent exclusion decisions are an intended objective for economic crime policy makers is explored in Section 4.3. of this study.

3.19. Is cross border information sharing permitted?

The majority of platforms surveyed are domestic only, however the Singapore platform stands out with regard to including design aspects which do consider cross-border information sharing.

In Singapore, the COSMIC platform proposal 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 FI's AML/CFT controls) and outsourcing of ML/TF/PF risk management operational functions."[63]

COSMIC permits such sharing of information they 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 will be required to comply with additional safeguards when sharing to individuals outside of Singapore and outside of the financial group, such as data anonymisation.

Salv stated in this study that they have conducted legal analyses to determine the basis for AML Bridge – not just in Estonia, but as a potential pan-European solution with work ongoing to explore the legal viability of a cross-border use-case within Salv AML Bridge.[64]

In terms of cross-border information sharing, fraud and ML may draw from progress in relation to cyber threat information-sharing. Under the Budapest Convention on Cybercrime, which supports a guideline for any country developing domestic legislation on cybercrime and as a framework for international cooperation between State Parties to this treaty. In particular, the Convention provides a legal framework for international cooperation on cybercrime and electronic evidence. Chapter III of the treaty makes general and specific provisions for cooperation among Parties "to the widest extent possible"[65] not only with respect to cybercrime (offences against and by means of computers) but with respect to any crime involving electronic evidence. It may be that due to the breadth of the Budapest Convention that it could support cross border collaboration between ECR platforms.

Section 4 – Summary analysis

4.1. Impact to date from private-private ECR information sharing

4.1.1. Private-private ECR information-sharing is providing value in identifying and mitigating risk.

To varying degrees, private-private platforms in this study are able to demonstrate:

- Improved detection rates of financial crime and greater discovery of subjects of interest;
- Faster speed of response;
- Reduction in the propensity for criminals to target participating institutions;
- In some cases, greater recovery of funds;
- Reduction in duplication of processes and cost due to pooled resources and shared value; and
- Reduction in risk displacement (for members)

The efficacy improvements from developing utility models for previously siloed activity are relatively straightforward to describe. Sharing a list of adverse incidents between market participants provides for more comprehensive visibility of those incidents compared to each market participant having to rediscover the same adverse activity. Being able to analyse transaction flows between participants allows for the discovery of linkages (and, crucially, the details of the linked accounts) between known high-risk accounts which may otherwise be sitting as fragmented data in different organisations.

Whether it is the billions saved through fraud domain platforms (described above), the identification of new targets of suspicion, or the speed of resolution of a query – platforms are able to show a range of promising performance data to highlight the value of private-private information sharing.

4.1.2. Stakeholders are achieving greater legal and regulatory confidence in the use of private-private ECR platforms.

Confidence in previously untested forms of sharing is growing, supporting greater clarity and confidence in the legal and regulatory basis for the respective innovation. In 2020 and 2021, many platforms have proved certain concepts related to the ability to link and analyse connected data and identify financial crime risk. Platforms have established legal grounds and greater clarity over the legal position of certain acts of sharing, where before the acts of sharing or the level of privacy preserving encryption had previously not been attempted or explored from a legal perspective.

4.1.3. Data inter-operability issues are being resolved.

A major technical challenge in previous years has been to support data inter-operability between financial institutions involved in platforms. Typically, major retail banks have considerable legacy IT issues, sometimes compounded by a history of takeovers that led to a bank's current form but with still operating a patchwork of IT systems. To achieve data inter-operability between such financial institutions is a major technical and data engineering exercise.

However, the growth of these platforms has demonstrated that even for large and mature retail financial institutions, data between financial institutions has been made inter-operable and the technology exists for relevant analytics and privacy preserving measures.

Developments explored in this study point to the maturity of the technology to be able to deliver the required capabilities. On the whole, technology is not a barrier to the development of this field, rather the issues rest much more in terms of policy issues, lack of clarity and conflicts.

4.1.4. GDPR is not, in itself, a barrier to ECR private-private sharing

Many of the platforms surveyed in this study operate in GDPR jurisdictions. While historically, GDPR has been raised as a considerable barrier to ECR private-private information-sharing, the growth of such platforms in GDPR jurisdictions should lead to a more nuanced dialogue on how best such platforms can fulfil data protection principles and what are the advantages and disadvantages of various legal bases under GDPR for such platforms.

4.1.5. ECR platforms have built up considerable experience in the governance frameworks and processes for strengthening trust in ECR platforms.

Bringing together multiple financial institutions or other regulated entities in a joint initiative takes a process of leadership and co-developed trust.

Parties often require a lengthy process in order to coalesce around an operating model and build the trust necessary to support ECR platforms. Many of the platforms surveyed have spent a substantial amount of time developing the governance process for the respective engagement and for each side to ensure that they have technical and legal confidence in the processes.

A large body of experience has been built up from supporting projects/pilots and initiatives to enhance private-private financial information sharing, including – the business case, algorithmic modelling, establishing a data model and initiate standards alignment, vetting of technology options, legal assessments, confirmation of models, data model and technology, evaluation of triggers for data sharing.

4.2. Key policy questions for policy-makers to engage with

The growth of private-private financial information sharing platforms raises a number of policy questions for financial crime stakeholders, principally because capabilities are enhanced.

This brings to the fore relatively fundamental questions for ECR policy-makers, including:

- Do governments really wish to exclude 'bad actors' from the financial system?
- Should there be a clearer legislative basis for denial of financial services for domestic criminality (domestic sanctions / blacklisting) and a robust governance process for such a determination?
- Should the subjects of financial crime risk assessments be made aware of those assessments and have an opportunity to challenge them?
- How far should platforms themselves offer an opportunity for data subjects to challenge the accuracy of information through an appeals process?
- What are the forms of redress or data correction available to data subjects who have been wrongly associated to financial crime risk?
- Should there be a regime which is similar to the credit rating agency process, whereby an individual can understand their financial crime risk 'score' and also take steps to improve their score?
- How long does financial crime risk 'stick' or be associated to an individual?
- If an individual has served a custodial sentence or completed an extremism de-radicalisation process, should financial crime risk still be associated to them? If not how can they become financially rehabilitated?
- In the absence of a subject appeals process, how does the platform and its members assure itself on data accuracy issues?
- What balance and thresholds of data shared, at what points in the spectrum of suspicion, should information sharing be permissible?
- If private-private ECR information sharing is adding value to the detection of economic crime, should it be mandatory?
- Should specific types of information or incidents be mandatory to share or make accessible to other regulated entities?
- What range of business sectors should contribute financial or business intelligence to support the discovery of economic crime, beyond traditional regulated sectors?
- How far should intelligence platforms across fraud, cyber and AML be connected?
- What threshold of data should be connected? Only alerted data or all transaction data?
- What privacy preserving technology should be used to provide greater security and reduced access to information during such processes?
- How can legal clarity for cross border information sharing be enhanced?
- With increased intelligence on economic crime risk, is the public sector able to process and act on such intelligence to deliver criminal justice outcomes?
- Should there be greater use of dedicated law enforcement units which are part funded by the platform members to deal with address the economic crime risk discovered by the platform?
- Should policy-makers encourage de-centralised information-sharing, rather than pooled or centralised sharing?

In the following section of this summary analysis chapter we provide further commentary on the issue of how platforms engage with the phenomenon of financial exclusion and the responsibility on policy makers to provide a clearer operating environment and overall policy intent with regard to financial exclusion.

4.3. Financial exclusion and engagement with the data subject

4.3.1. Recognising the lack of policy clarity on financial exclusion as an objective.

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 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".[66]

This topic is a complex one, but - in essence - the entire AML framework encourages individual regulated entities to make account closure decisions in isolation and in an uncoordinated way. The historic situation whereby client exit decisions are common but uncoordinated is generally ineffective in disrupting serious and organised crime (as serious crime networks can maintain vast networks of accounts to support their ML objectives). However, from a policy perspective, the ineffectiveness of account closures at a system-wide level somewhat alleviated pressure about the need to have a clear position as to whether financial exclusion for high-risk entities is desirable and intended or not.

Without private-private information-sharing, the decision can be devolved to individual firms making 'risk-based decisions' about who they wish to provide commercial services to. However, the prospect of more consistency between regulated entities in who is denied services brings a policy conflict into sharper focus as to whether there is a right to financial services and 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.

Platforms offer capabilities to provide more consistent denial of services to high-risk entities, but it is not clear that the outcome of a set of citizens being denied financial services is a desirable outcome. More consistent account denial may create a class of individuals who would be forced into underground banking and there may be negative implications in terms of the loss of financial intelligence value associated to reporting on such high-risk entities (were they to hold accounts within the regulated sectors). It is also not clear if it can be justified to entirely exclude citizens from financial services on the basis of suspicion alone and outside of a judicial process.

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.

Platforms should operate under greater certainty about whether the overall policy objective is to exit high-risk accounts or have them subject to more intensive monitoring. They can be used to achieve either objective more effectively.

4.3.2. Recognising the need for data correction and providing an opportunity for redress to the data subject.

Cifas is the only platform surveyed in this study which actively supports a review and appeals process for data subjects, in addition to a review process undertaken by the member.

The proposal for Singapore COSMIC requires that financial institutions, in their risk assessment around a client exit procedure, should contact the customer and provide them with "adequate opportunity to explain the observed activity."[67]

It is reasonable to infer that false positives will make their way into a private-private ECR information sharing platform. Without a process for challenge, coming from the data subject themselves, it will be difficult for the system to ensure data accuracy as well as procedural justice for citizens. A negative record with regard to financial crime risk may see individuals in a very challenging situation of not being able to access essential public services or engage in fundamental aspects of society by not being able to maintain a financial account.

Notwithstanding the value of information sharing, the routes of data correction and appeals for data subjects must be adequate and allow for an individual who is wrongly associated to 'risk' within an information-sharing framework to challenge that designation.

Section 5 – Enabling themes for private-private ECR information-sharing platforms

Policy-makers and private sector stakeholders may wish to enhance the overall operating environment for private-private ECR information sharing platforms.

In the following section, drawing from a wide range of insights that have been raised by project managers through the interview and broader research process for this study.

We have framed these insights for policy-making around three key enabling themes for ECR information-sharing platforms, and 15 contributing factors that support those themes.

- **Theme 1.** Shared strategic vision between public and private sector stakeholders.
- **Theme 2.** A clear enabling legislative and regulatory environment.
- **Theme 3.** Robust governance, data ethics and accountability.

Theme 1. Shared strategic vision between public and private sector stakeholders.

A shared public and private sector strategic vision should be established for the role different sectors in relation to responding to economic crime related threats; the desired capabilities for identifying and responding to economic crime threats; and, accordingly, clarity on the information-sharing and connectivity requirements to fulfil those capabilities.

To support this theme, we highlight issues both at the national level and the international standards level, covering the following **6 contributing factors**:

1.1. Leadership, trust and shared objectives.
1.2. Commitment to data integration.
1.3. Law enforcement engagement.
1.4. Clarity over the intended treatment of the data subject.
1.5. Joint endeavours to promote public acceptance and a 'social licence' to operate.
1.6. International-level unambiguous support within relevant standards (FATF).

5.1.1. Leadership, trust and shared objectives.

Platform project managers emphasised the importance of leadership, confidence building and shared objectives as foundational to the success of an ECR platform initiative.

Leadership from public and private sector stakeholders sets a 'tone from the top' to encourage information-sharing and has been raised as essential for platforms to achieve the necessary support, 'buy in' and critical mass.

Leadership engagement can be established through clear policy commitments or 'action plans', which include the involvement of both public and private sectors.

Case studies

UK high-level public-private sector collaboration and leadership to the response to economic crime

The "UK Economic Crime Plan 2019-2022"[68] is viewed as positive examples of such a process and the UK Economic Crime Strategic Board provides a very positive example of senior level leadership engagement from public and private sectors.[69]

The Economic Crime Plan itself was the product of a wide ranging consultation process and builds from the UK's 7 priority areas for reform which were published in January 2019, covering the need to:

1) develop a better understanding of the threat posed by economic crime and our performance in combatting economic crime;
2) pursue better sharing and usage of information to combat economic crime within and between the public and private sectors across all participants;
3) ensure the powers, procedures and tools of law enforcement, the justice system and the private sector are as effective as possible;
4) strengthen the capabilities of law enforcement, the justice system and private sector to detect, deter and disrupt economic crime;
5) build greater resilience to economic crime by enhancing the management of economic crime risk in the private sector and the risk-based approach to supervision;
6) improve our systems for transparency of ownership of legal entities and legal arrangements; and
7) deliver an ambitious international strategy to enhance security, prosperity and the UK's global influence.

The delivery of the plan is overseen by the Economic Crime Strategic Board which brings together the Home Secretary and Economic Secretary to the Treasury, together with other relevant Ministers, senior leadership from relevant public regulatory and law enforcement agencies, Chief Executives from a wide range of major regulated entities.

At the operational level, public and private sector trust, coordination and confidence building has evolved in line with the development of the UK Joint Money Laundering Intelligence Taskforce and the UK National Economic Crime Centre (NECC). On October 2018, the UK launched the NECC within the NCA, which includes representation from the UK FIU, City of London Police, Serious Fraud Office, Financial Conduct Authority, Home Office, Crown Prosecution Service and HM Revenue & Customs. The multi-agency centre has responsibility for planning and coordinating the operational responses across agencies, with the stated intent to bring together the UK's capabilities to tackle economic crime more effectively. The NECC has a mandate to define a set of national financial crime priorities, with supervisor and law enforcement support, and FIU and private sector engagement.[70]

High-level public-private sector collaboration and leadership to the response to economic crime in the Netherlands

The Netherlands also benefits from a clear public-private strategic dialogue framework and published Action plan.

The Netherlands established the 'Financial Expertise Centre' (FEC) as a central national public-public coordinating authority, with oversight of cross-government coordination on financial crime and oversight of all national public-private financial information sharing partnerships. The FEC is a cooperative association of the Netherlands Authority for the Financial Markets (AFM), General Intelligence and Security Service, Tax and Customs Administration, De Nederlandsche Bank (DNB), Fiscal Intelligence and Information Service and Economic Investigation Service, Public Prosecution Service and the Police Force.

In 2019, the Dutch Ministers of Finance and Justice and Security submitted a "joint action plan for the prevention of money laundering through the Dutch financial system and for tracking and prosecuting criminals and their enablers" to the Dutch parliament.[71] The 2019 Dutch 'Joint Action Plan', with a suite of over 40[72] specific actions, committed to the regular execution of National Risk Assessments to support policy making and called for cross-government collaboration to be reinforced through the national 'Financial Expertise Centre' to understand threats and share trends across the range of relevant agencies.[73]

The plan set out a strategic intent to support various forms of sharing information, including increasing the effectiveness of joint transaction monitoring by banks by means of a "TM utility". The plan specifically highlights that the value of a transaction monitoring approach will be more effectively realised when participants are able to analyse flows across multiple institutions, rather than to view transaction data only in silos of individual financial institutions. The strategy also supports the development of public-public information sharing by increasing the scope for AML regulators to share information with bodies within the Financial Expertise Centre (FEC).[74]

It is not surprising perhaps that the UK and the Netherlands collectively host a substantial number of the ECR platforms covered in this survey.

Platform managers have raised the importance of building momentum and achieving consensus towards shared objectives, but without a strong public-private sector strategic architecture for responding to economic crime, this can be very difficult.

With regard to the platforms themselves, a clearly defined set of objectives for the information sharing and a performance measurement framework around those objectives should underpin the success of the platforms.

Ultimately, the growth of private-private ECR platforms provides policy makers and practitioners with enhanced capabilities to address economic crime risks. Achieving clarity on the capabilities that policy-makers wish to see in operation will materially affect the design considerations around the type of information sharing which is permitted and the legal and regulatory framework around that.

Legislation that allows one type of collaboration may or may not support another capability. As such, policy makers should reflect on which of the following capabilities they wish to see in operation and design a policy framework that supports the relevant objective, including:

A. The development of economic crime threat typologies.
B. Adverse incident databases.
C. Messaging communication (queries and responses).
D. Transaction monitoring for alert generation for new risk and patterns based on analytics of combined data.

E. Collaborative intelligence and investigations by members.
F. The development of evidence packs for law enforcement by a private-private platform.

Policy makers should be clear about what capabilities they wish to see in operation and how relevant data can be best connected, underpinned by clear regulatory and legal support for such information-sharing processes.

5.1.2. An overall commitment to data connectivity

The second contributing to factor to this theme is the existence of a high-level policy commitment to improve connectivity between relevant data sources and breaking down silos of fragmented data relevant to identifying economic crime risk.

This commitment should flow from the overall set of policy objectives, described in the first contributing factor, but specifically address the problem of different types of data silos, including:

- Public and private sector data connectivity.
- Fraud and AML data.
- Connections between platforms.
- Connections across different sectors.
- Better utilisation of payments data.
- Carefully calibrated thresholds for input data to ECR platforms.
- Connectivity with digital identity processes and data.

Commentary on achieving connectivity between these different data silos are described below:

1.2.1. Public and private sector data connectivity

Certain public sector departments and agencies can have a large amounts of data on fraudulent events which could usefully be connected to private-private ECR platforms.

Greater sharing of data, intel and learning - particularly by central government stakeholders - can form part of the high-level commitment to better connectivity between relevant data sources. In particular, platform managers described how government efforts to identify fiscal or welfare fraud could be better connected with private sector efforts to determine ECR risk.

ECR private-private platforms are ultimately providing a public good, but even in jurisdictions where ECR platforms are thriving there is not a clear and concerted effort by the public sector to support the functioning and effectiveness of those platforms with relevant data.

1.2.2. Fraud and AML data.

Overall, project managers report that there is substantial cross-over in threat between fraud and money laundering networks, but - in most jurisdictions - there is a stymied response due to legal environments that have evolved in entirely separate frameworks. Economic crime risk awareness is being undermined by siloed approach to fraud and AML. This survey has demonstrated that there are numerous ways in which learning may be able to cross over between fraud systems and AML systems (and vice versa).

As with the cross over with fraud and AML, cyber enabled threats and ML and fraud threats are overlapping and have a complex inter-relationship. The awareness of risk in one domain will likely support awareness of risk on another domain.

An overall commitment to data connectivity should explore how fraud, cyber and money laundering threat data can be better integrated and made available for collective analysis.

1.2.3. Connections between platforms.

While some platforms support inter-connectivity and syndicated access to respective data, platform owners raised a challenge that there was a wider a lack of public policy support and strategic thinking with regard to being able to connect data platforms that support analysis of ECR risk. Syndicated or metered access opportunities could be achieved to ensure that financial crime insight and awareness was not fragmented and siloed in sectoral information-sharing initiatives.

Even in jurisdictions, such as the UK, where numerous ECR platforms exist, the platforms can tend to operate without a strong connection to one another. Financial institutions or other users of platforms must still engage with and draw from multiple platforms. As a result, there may be limitations in the discovery of financial crime risk because of the inability to see linkages between insights that are available in respective platforms.

Underneath a broader strategic approach to addressing economic crime, there is an opportunity to provide support for greater connectivity between existing ECR platforms. The opportunity to achieve such connections would materially enhance the effectiveness of the national response to economic crime threats, and as such should be considered by jurisdictions at the policy level.

1.2.4. Connections across different sectors

Silos of data relevant to economic crime risk often exist between different commercial sectors. This can be because different sectors have developed different ECR platforms, or it may be that a particular sector has not yet engaged in existing ECR platforms.

Part of the overall strategic response to economic crime should ensure that there is a clear vision for how better connection can be achieved between financial crime risk data across different sectors. This may include sectors that are outside of the traditional money laundering regulated sectors, but still have relevant data for identifying economic crime risk – such as integrating telco, social media and ISP private sectors into overall efforts to disrupt economic crime.

1.2.5. Better utilisation of payments data

Payments data is a natural centralised data source for financial behaviour which can be used to understand networks of criminality stretching across multiple financial institutions. The Vocalink platform described in this study is one example of successful analytics applied across payments data. However, in general payments institutions have not been subject to money laundering regulations or heavily engaged in public-private financial information sharing.

An overall commitment to enhance connectivity of financial data - and ensuring economic crime risk analytics has the best possible coverage over connected data - should include consideration about how both traditional and non-traditional payments data can be incorporated into the national response and ECR platforms.

1.2.6. Carefully calibrated thresholds for input data to ECR platforms.

The strategic commitment to better data interconnectivity in the economic crime risk response should seek to ensure that the thresholds for input data to ECR platforms are appropriately set.

UK case study – miscalibration of input data thresholds.

In the UK, historically, private-private financial information sharing appears to have been limited by a miscalibration of thresholds and an overly cumbersome reporting process, adding cost, complexity and potential penalties to the act of information-sharing.

UK private-private information sharing was supported through the information sharing provisions in POCA section 339ZB to 339ZG (as inserted by the Criminal Finance Act (CFA)2017). However, in the CFA 2017, the threshold for private-private information sharing was widely believed by regulated entities to be set too high; i.e. at the standard of 'suspicion', whereby a (first) regulated entity will have already met the threshold to file an individual suspicious activity report. As a result, the use of the Criminal Finances Act 2017 mechanism for private-private sharing has been extremely limited since its establishment.

Setting the threshold for ECR private-private information sharing is a key policy consideration.

As with the UK example, setting the threshold too high can negate the use of the mechanisms. However, too low a threshold may not be acceptable from a data protection perspective.

A lower threshold opens up the opportunity for broader data analytics, while a higher grade of concern (or initial alert) will minimise the data sharing occurring.

1.2.7. Connectivity with digital identity processes and data

The overall approach to data connectivity should ensure that public sector and private sector efforts to provide a framework for digital identification and validation of identity can be linked to economic crime risk analysis.

5.1.3. Law enforcement engagement.

In terms of end-to-end effectiveness, a number of platform owners described challenges in terms of the lack of visibility of law enforcement action on the identified criminality and the sense that the ECR platforms were engaged in a continual 'whack-a-mole' process without truly disrupting the underlying organised crime activity.

Project managers from ECR platforms, particularly from fraud-domain platforms, report that while a false identity can be disrupted, or 'burned', the criminal network does not then give up criminality. Instead, criminal parties are observed to attempt new methods of economic crime or develop new false identities.

Lack of public sector responses to intelligence produced by the private sector was a common feature in challenges described by both fraud and AML domain platform owners.

The majority of ECR private-private platforms surveyed do not have a strong or central link to a public agency or an enforcement arm that is resourced, motivated and directed to take action to disrupt or dismantle a relevant criminal network.

To achieve a greater effect against the underlying criminality, there is a need for public-private and private-private information sharing to link more effectively together.

However, platform managers highlighted that there was often a recognition that criminal justice systems are not likely to be able to cope with the volume of economic crime. Private sector detection of financial crime risk could risk (or is) 'swamping' the public sector with leads of criminality.

In order to stem the flow of economic crime, a more strategic approach is required which take a blend of disruption, deterrence, prevention, target hardening, education, and rehabilitation.

The need for (some level of) credible law enforcement action on the intelligence produced by ECR platforms and the need to recognise the limitations of that law enforcement response and plan for other forms of 'action' against relevant subjects is a key issue to address in order to ensure that resources and capabilities within ECR platforms are utilised effectively and efficiently.

5.1.4. Clarity over the intended treatment of the data subject.

Project managers of ECR platforms described the current framework for 'action' in response to economic crime risk as relatively 'blunt', particularly with regard to account closures by individual regulated entities.

ECR platforms can help support a more clinical and precise treatment of subjects, in place of the reliance on uncoordinated account closures.

For example, 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.

The AML regime has historically been focused on individual regulated entities and a firms' risk management, but ECR platforms offer an opportunity for the overall system to be much more centred on the subjects themselves. ECR platforms should be consider their role in providing a pathway for data subjects – following criminal justice processes, or given the absence of the original offending behaviour - to be rehabilitated or reintegrated into financial services and society more generally.

5.1.5. Joint endeavours to promote public acceptance and a 'social licence' to operate.

As part of the mission of this theme to achieve a strategic vision for the role of private-private information sharing to respond to economic crime in society, there needs to be public acceptance of the role of private-private information sharing to detect crime.

As such, ECR platforms need to be supported by government and private sector communications about the value and importance of this activity.

In a number of situations, private sector stakeholders raised the need for a broader and stronger level of public and political support for the function of the private sector in terms of identifying criminality through collaborative analytics.

It was raised as a concern that without strong and cross-party support for such activity, the role of platforms could be undermined or politicised in the future.

5.1.6. International-level unambiguous support within relevant standards (FATF).

Despite the evidence of positive impact of ECR platforms, there is no clear policy support for private-private sharing at the international standards level for FATF.

In a major contribution to advancing the international standards engagement with private-private information sharing, in July 2021, FATF - the international standards setter for the AML/CFT regime - published a 'Stocktake on Data Pooling, Collaborative Analytics and Data Protection'.[75]

However, at present there is no clear and unambiguous support for private-private ECR information sharing within the FATF international standards. As such, national governments must reach beyond international standards to achieve the enabling themes set out in this report.

A large number of countries may be reticent to take such policy action, in the absence of support or recognition from FATF.

FATF should evaluate whether ECR private-private sharing platforms are providing value to the identification of crime risk, and, if so, provide a more supportive framework for their growth within the standards.

FATF also have a key role in many of the other recommendations in this paper, including achieving greater clarity with regard to the objective of financial exclusion, the integration of fraud and AML approaches, and standards to guide how long individuals are associated to economic crime risk for example.

Theme 2. A clear enabling legislative and regulatory environment.

If policy makers have a shared vision with their respective private sector and a clear set of objectives and capabilities that they wish to see deployed to respond to economic crime threats, then there is a need to ensure that the policy environment is fit for purpose to support those objectives.

We draw together insights shared relevant to this enabling theme under the following **two contributing factors:**

2.1. Policy commitment to achieve legal clarity on the required information sharing, taking into account obligations under relevant privacy statutes, competition law and safe habour from liability and defamation.

2.2. Regulatory clarity from respective data protection, competition law and AML supervisors that such information-sharing is permissible and desirable, with relevant guidance available.

5.2.1. Policy commitment to achieve legal clarity on the required information sharing, taking into account obligations under relevant privacy statutes, competition law and defamation.

Particularly in the AML domain, without clear enabling legislation, collaborative analytics and platforms surveyed in this study tend to be limited to slices of data which are exempt or more clearly justified under GDPR, for example: business client data; pilot exercises to test GDPR and public interest as a basis for processing under GDPR; a fraud focus; or ATM data for example.

This survey demonstrates that GDPR can support information-sharing for fraud prevention purposes, but is a poor legal framework to support AML domain information sharing.

In any jurisdiction, there can be countervailing disincentives to information-sharing. If a government wishes to encourage ECR information-sharing it will need to provide legal clarity – not just that ECR information is protected from civil liability – but also that participants will not be in breach of data protection regulation, competition law and AML regulatory risk associated to tipping off.

The precise legislative requirement will depend on the determination of a shared strategic vision, described in theme 1, including for instance: the objectives and desired capabilities of an ECR platform, the extent to which fraud data is to be integrated with AML data, the desired level of financial exclusion for subjects of economic crime risk, the range of sectors that are desired to be part of ECR information sharing, the thresholds for input data to ECR platforms and any purpose limitation that is deemed appropriate.

As an international example, the Dutch AML Action Plan was accompanied with the publication of government research paper reviewing the Dutch legal regime as a whole in the context of the AML Action Plan. The study highlights what is currently possible within the law, what reforms would be required to achieve the ambition of the AML Action Plan, and also highlights the design conditions required to be compliant with data protection and competition law.

Without the appropriate legal clarity, the resulting ambiguity will deter regulated entities from engaging in information-sharing, despite the effectiveness advantages, due to the fear of associated legal or regulatory risk (from a privacy, competition, civil damages or anti-tipping off perspective, for example).

5.2.2. Regulatory clarity that such information-sharing is permissible and desirable.

It will be important for policy-makers to take responsibility for achieving a 'whole of government' view on the appropriateness of ECR private-private information sharing and engage in a process to identify and resolve any potential challenges in relation to the intersection with the set of relevant regulatory regimes.

In addition to policy and legal clarity on ECR information-sharing, there will need to be consideration given to regulatory guidance (from the relevant regulatory regimes), the publication of model impact assessments or support for codes of practice which assist regulated entities to fulfil their requirements under each regulatory regime while still achieving the desired state of ECR information-sharing.

AML supervisors will need to set a expectation that ECR private-private information-sharing is a desirable activity and is relevant (in a positive manner) within the supervisory examination process.

Historically, the majority of AML supervisors have not sought to encourage private-private ECR information sharing, nor regarded it explicitly as a means to ensure more effective results for the AML/CFT system as a whole.

In the UK, the HM Treasury 'Review of the UK's AML/CTF regulatory and supervisory regime' from July 2021 aims to address these issues. In the U.S., the principal AML supervisor, FinCEN, takes clear steps in public communications to "strongly encourage" financial institutions to participate in 314(b).

In Singapore, the Monetary Authority of Singapore, as the AML supervisor, makes clear in the most recent proposal to support private-private AML information sharing that:

> *"[When] FIs are not permitted to warn each other about potentially suspicious activity involving their customers…. each FI's understanding of their customers' risk profile is limited by the information the FI collects. Criminals have been able to exploit this weakness by conducting transactions through a network of entities holding accounts with different FIs, such that each FI by itself does not have sufficient information to detect and disrupt illicit transactions in a timely manner. Allowing FIs to share information on customers that cross certain risk thresholds enable them to break down these "information silos" and more effectively detect and disrupt criminal activities, reducing any harm done to the integrity of Singapore's financial centre."*

In addition to AML supervisors, regulatory clarity should also be provided from respective data protection and competition law supervisors that such information-sharing is permissible, with relevant guidance available.

Theme 3. Robust governance, data ethics and accountability.

Given a shared strategic vision and an appropriate legislative and regulatory environment for ECR private-private information sharing, our final enabling theme refers to the processes of governance, data ethics and accountability which should support the safe and ethical long-term development of this capability.

We draw together insights within this enabling theme under seven contributing factors:

3.1. Robust governance
3.2. Sustainable funding
3.3. Governance advantages of a central platform
3.4. Cyber-security, information security, operating procedures and professional standards
3.5. The use of technology to enable information-sharing and data ethics
3.6. Privacy preserving analytics
3.7. Performance management and reporting

5.3.1. Robust governance

As a nationally significant financial intelligence and crime deterrence, investigation and prevention capability, ECR platforms will require adequate governance structures to support their objectives, achieve accountability and manage various risks.

A number of platforms surveyed in this study operate under clear operating procedures and members face obligations and standards of practice to participate in the platform.

As the level of public support for ECR private-private platforms grows, so too should the level of governance.

Key questions for governance design include:

- Who owns the private-private sharing platforms?
- Who is accountable for the management of the operational risks and service levels of the platform?
- Who manages liability for any regulatory or legal risk associated to the information-sharing?
- Who is accountable for any damages caused by the use of information held by the platform?
- How will the future direction and investment roadmap for the platform be managed?
- What will be the criteria for participation and / or exits from the platform?

Even in public-sector led initiatives, private sector involvement at the governance level will be important to ensure it stays connected to the realities and needs of the members. Apart from ensuring strong and robust governance around the platform. Platforms will need to focus on adding-demonstrable value to both the public and private sectors on an ongoing basis to preserve the support it benefits from now going forward.

Challenges in relying on only a legal gateway, without robust governance for the information-sharing
Case study: Traditional use of 314(b)

The USA PATRIOT Act 2001 supports private-private sharing through section 314(b) by "provid[ing] financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report activities that may involve money laundering or terrorist activities." 314(b) provides the widest scope for economic crime related private-private information sharing out of any comparable jurisdiction, covering a wide range of predicate criminal activity and affording clear safe harbour from liability.

This legal gateway perhaps provides the best example of information-sharing which is devolved entirely to the private sector, without – historically – substantial engagement from the public sector or substantial attention to the governance processes around information sharing.

However, for most of the legislative lifetime of 314(b), information-sharing through 314(b) has been limited. Platform project managers raised a number of obstacles or limiting factors for use of 314(b) over its legislative lifetime, including:

- Lack of trust and confidence about whether 314(b) requesters may be mis-using 314(b) to discover client relationships of the requested institution.
- Some larger financial institutions stated in FFIS workshops that they believed that smaller financial institutions should not be using 314(b) at the stage of onboarding a client – this was described as 'outsourcing KYC requirements' – and was believed (by some stakeholders) to be inappropriate use of the mechanism. However, whether 314(b) can or should be used at the onboarding process and to support KYC processes remains a point of contention between different 314(b) users. As such, lack of consensus around purpose and achieving purposes limitation may be undermining elements of the effectiveness of 314(b) ECR information-sharing.
- At its most basic level, 314(b) relies on a 'clunky' secure email platform for information exchange and has been described as burdensome for a requesting entity to discover whether the desired recipient of a query is registered for 314(b) and can, therefore, legitimately receive a 314(b) request through an appropriate point of contact. While technology has moved on to support platform-based exchanges, this has only occurred relatively recently since the mid- 2010s as a development in 314(b) practice and norms.
- As a result of the clunky and decentralised nature of information exchange under 314(b), there are no generally accepted standards in the data format of both queries and responses – bringing in inefficiencies and challenges drawing in subjectivity about whether a request has been adequately formed or whether it is complete.
- 314(b) information-sharing in the U.S. has been affected by challenges of long delays in response times (some participants refer to 'months') and some queries are not responded to at all.

However, it should be noted that while the legal gateway of 314(b) does not come with in-built governance or oversight of particular exchanges, a number of the 314(b) based platforms surveyed in this study have established robust governance procedures to establish the standards of member behaviour and the operating procedures.

5.3.2. Sustainable funding

In addition to robust governance, ECR platforms require a sustainable funding model.

While many of the platforms surveyed are commercial and for profit, others are member funded non-profits, and a number represent pilots without a sustainable model of funding.

Platform designers should consider how the broader vision for addressing economic crime risk, in particular the funding of the law enforcement action to follow-up on the output of the platform, can be established in a sustainable manner.

Drawing from the example of the UK insurance industry's connection with the City of London Police IFED, other sectors and platforms should consider closer relationships with dedicated law enforcement units and funding arrangements for such units.

In the UK, a new levy on industry is being established to support more robust funding of the National Economic Crime Centre to support more effective capabilities which can also serve and support interest of financial integrity more effectively. However, it is yet to be seen whether the new levy will provide funding support to UK private-private ECR platforms.

5.3.3. Governance advantages of a central platform

To support effective data governance, ideally there should be a central platform, rather than simply a legal gateway for bi-lateral and ad-hoc messaging (as described in the traditional use of 314(b) messaging above)

Interactions in the platform should be tracked, logged, and stored with a tamper-proof audit trail. There is a strong governance and accountability argument for ensuring that the entire information sharing history, including related notes and files, should always be available for auditing and reporting.

However, it should be noted that the use of privacy preserving analytics may challenge some of these processes and indeed the viability of auditing processes. Several of the platforms surveyed in this study have no access to or retention of the data.

Having a centralised platform for information-sharing allows for a large number of advantages, including:

- Case management
- Multi-party involvement in messaging or investigations collaborations
- More comprehensive performance management
- Standards of timeliness in the response
- The ability to push notifications for risk to the member
- Greater standardisation of formats of requests and responses
- The opportunity for audit and simplified reporting of the interaction.
- Link analysis of connected entities discovered by multiple participants in the platform
- More efficient capture and transfer of information related to a case as a whole, such documentation and file attachments (e.g., loan applications, signature cards, surveillance videos, identification, payroll statement, etc.) accessible within the case in preparation for the final output of reports to law enforcement.
- The potential for audit of compliance with any threshold conditions on information-sharing.
- The standardisation of operational routines, data standards, formats and quality.
- Audit and inspection of data holdings
- The ability to correct data over time
- The ability to support a data correction appeals process in relation to the data subject.
- The ability to track back to law enforcement outcomes to identify false positives, false negatives and enrich true positive hits.
- Ongoing curation, de-duplication of records, quality assurance and overall service management of the data.
- Openness to inspection by data protection agencies
- If limitations exist on the type of data that may or may not be shared, this can be incorporated int structured data fields.

- Greater assurance that platform users are compliant with regulatory expectations and guidelines for sharing information.
- Greater opportunity to achieve consistent definitions of suspicious or ECR activity
- Platforms will contain highly confidential data and appropriate security governance, physical access to data, authentication and authorisation to systems needs to be put in place to ensure the system is monitored and controlled.

5.3.4. Cyber security, information security, operating procedures and professional standards

Governance processes will need to mitigate against cyber security and information-security risks.

As a 'honeypot' of information and given the relevance to disrupting organised crime, ECR platforms may expect to be under significant pressure in terms of cyber security attacks, infiltration and corruption attempts from stakeholders as diverse as organised crime, kleptocrats and malign state actors.

As such, an increasingly important issues for platforms and members will be the information-security and personnel security obligations of membership.

Currently platforms demonstrate a number of different approaches to ensuring standards in the area of information-security and operating procedures. Standards in this area and validation, audit and compliance processes are likely to require strengthening as capabilities develop.

5.3.5. The use of technology to enable information-sharing and data ethics

The use of technology and breaking new ground, particularly in terms of data inter-operability and use of privacy preserving analysis, are hallmarks of more recent ECR private-private platforms.

In many ways, developments in technology have underpinned the opportunity for ECR platforms to flourish and also put pressure on the adequacy of older models of processes for identifying and reporting financial crime risk.

ECR platforms, at their heart, enable a far more efficient discovery of financial crime risk by being able to surface financial crime risk spread across multiple institutions and reduce duplication of effort by centralising some aspects of the identification process.

However, very few of the platforms surveyed in this study are yet making full use of the potential of machine learning.

Platform owners raised the importance of allowing for a maturity development of private-private financial information sharing and making use of advanced analytics techniques.

As part of an enabling environment for the growth of ECR platforms, key public and private sector stakeholders should provide an opportunity to pilot, test and develop technological solutions to enhance the efficiency and efficacy of ECR platform processes.

The process of ensuring legislation and regulatory guidance are fit for purpose should also engage with the future potential development capabilities for private-private sharing and defining and resolving potential challenges from a privacy or model ethics perspective.

Particularly in the context of advanced analytics and machine learning, there will be a need to ensure that individuals are not targeted for profiling based on associations which would be in breach of anti-discrimination laws or other bias. There may need to be a broader public debate about what identifiers are legitimate in terms of understanding associations to financial crime risk. For example, whether a postcode / zipcode is a legitimate data point to use for associations for financial crime risk. We understand that postcode / zipcode associations are currently used by some industry stakeholders.

Many of these issues will not be able to be resolved by ECR platforms in isolation, but will require engagement from AML and data protection supervisors.

To continue to achieve efficiency gains and to support growth through the maturity curve, there will need to be a spirit of public-private collaboration in innovation and working through relevant technical issues.

5.3.6. Privacy preserving analytics

Only a minority of the platforms surveyed make use of privacy preserving analytics to limit exposure of information and maximise analytical or computational processes.

The connection between ECR information-sharing and privacy preserving analytics appear to be at an early stage.

To date, ECR platforms are finding benefits in privacy preserving techniques as follows:

- To allow for data to be held by a central utility and for transactional flow network analysis to take place without the central utility having access to relevant underlying data.
- Alternatively, to allow for data to be decentralised.
- To allow for messaging security to be enhanced and reduced disclosure in the query process.
- To allow for queries to be issued and (instant) responses received on pre-authorised sets of queries without having to disclose the query to the requested party.
- To allow for subjects of investigations to have their privacy and reputations protected, especially if only based on suspicion (vs confirmed criminality).
- To open a path to automated information sharing.

However, the growth of privacy preserving analytics will raise a number of issues that will require consideration at a more strategic level in order to create a conducive environment for growth of ECR platforms, these will include:

- Visibility of the extent of information sharing taking place at the central platform level.
- The opportunity to observe and discover data quality issues if input data is subject to privacy preservation.
- The viability of audit and compliance processes with operating standards.
- The opportunity to explain suspicion if privacy preserving techniques had alerted an organisation but without providing relevant underlying details.
- The opportunity for a data subject to understand if they have been processed (if the processing organisation itself does not have visibility over who has been processed in a macro level analysis)
- Understanding the correct process and points for data correction.
- The coherence with requirements for AML record keeping to explain decisions that have made use of privacy preserving data, where trust is with the system that provides an indication of risk, rather than in an ability to have the original source documents and take steps to investigate that information directly.

The balance of security and privacy benefits, and utility and particularly audit and inspection limitations through the use of privacy preserving analytics will likely be a major technical and platform design consideration in future years.

The role of both AML and data protection supervisors, and relevant industry codes of conduct, to provide greater clarity will be important to support progress in this field.

5.3.7. Performance management and reporting

A large number of platform project managers raised performance data as a key challenge, principally because:

- Members may fail to measure and report back to the platform the impact associated to use of the platform.
- The value of risk management benefits achieved through use of the platform can be difficult to quantify.
- The full impact of identifying criminality through private-private financial information sharing platforms is determined, in part by the take up by law enforcement authorities of disruption or criminal justice outcomes arising from intelligence. For a large number of the platforms surveyed, feedback on law enforcement outcomes can be negligible or limited.
- For fraud, in particular, some interviewees indicated that there can be an under-reporting of fraudulent activity due to institutional embarrassment, other reputational concerns or lack of actionable intelligence to share with law enforcement.

More work is required to develop techniques for measuring the performance of private-private sharing, including with regard to:

- Improved detection of financial crime risk and greater discovery of subjects of interest (private and public).
- Illicit assets restrained and recovered.
- Reduction in duplication of processes and cost for pooled activity.
- Reduction in risk displacement (for members).
- Evidence of reduced propensity to report activity (including lower false positives or greater discovery of false positives).

Understanding how ECR sharing can resolve and explain away concern

A key point of value in private-private information sharing is the potential for such sharing - particularly pre-suspicion messaging capabilities - to resolve concern and explain away behaviour with the benefit of counterparty information. This type of outcome data would be highly relevant and useful for understanding the wider impact of private-private sharing.

In the AML domain an ongoing challenge is the rising numbers of suspicious reports and growing data collection footprint on society of the AML regime, large proportions of which are deemed to be not useful to law enforcement investigations. The extent to which ECR information sharing can resolve false positives is a key point of value, but measuring its extent is more difficult.

Messaging has both opportunities to allow participants to receive a greater understanding of risk (causing reporting to increase), or may help explain behaviour and resolve concerns (exerting a downward pressure on the reporting). As yet, the balance of outcomes is not well understood in practice due to limited performance data

Measuring performance is a key area where ECR platforms can develop, including - ideally - with engagement from public sector agencies to achieve visibility over how intelligence developed in ECR platforms is contributing to outcomes from a criminal justice perspective.

With this whole-of-system and public-private approach to performance monitoring, policy-makers, supervisors and private sector stakeholders can better understand the contribution of ECR platforms to outcomes and, with such performance information, they can evaluate and assess how to further increase the effectiveness and efficiency of the national and international approach to tackling economic crime.

Conclusions

Overall, the driving impetus for supporting more effective ECR private-private information sharing is that the threat of economic crime is severe, but the response to the threat is inadequate and fragmented.

The threat is linked across money laundering, fraud, cyber and other forms of payment and assets, but both public sector and private sector responses tend to be siloed between and within each other and across the respective domains of economic crime. Collaborative analytics has a greater chance of detecting the underlying criminal behaviour and can produce substantial efficiencies and effectiveness gains compared to each private sector entity acting in isolation.

This survey indicates that the use of collaborative analytics through ECR platforms is growing, but platforms themselves have wide variance in practice and form.

Now is an appropriate time for policy makers to consider a more strategic approach to encouraging and co-designing the capabilities of private-private ECR platforms into a joined-up public-private strategy. Such a strategic approach can calibrate the capabilities and data threshold requirements in line with the operational requirements to respond to economic crime threats.

Even in more limited forms of input data, ECR platforms offer capabilities that should be supported in a more active manner by standard setters, policy-makers and supervisors. However, in tandem, private-private ECR platforms will have greater responsibilities to ensure the governance, accountability and data ethics of their processes if there is to be greater support from public agencies in terms of follow-up, contributing data and supervisory recognition.

In this paper we argue that, collectively, public and private strategic collaboration in the development of ECR platforms should be:

1) Encompassed within a **shared strategic vision** between public and private sector stakeholders for how economic crime is addressed, with clarity about the respective function and information-sharing requirements of both public and private sectors. This vision should include an overall commitment to data connectivity, it should recognise the extent of capacity of law enforcement engagement to respond to the threats and address how the remaining threats should be handled, it should take responsibility for how subjects of concern should be treated (including clarity over the use of financial exclusion as an objective), and should be underpinned by joint strategic communication endeavours to promote public acceptance and a 'social licence' for the platforms to operate.

2) Delivered through a **clear enabling legislative and regulatory environment,** with both a policy commitment to achieve legal clarity on the required information sharing and supervisory clarity that such information-sharing is permissible and desirable (taking into account data protection, competition law and AML regulatory regimes).

3) Developed with a framework of **good governance, data ethics and accountability,** including sustainable funding, attention to cyber security risks, adequate information security standards, operating procedures and professional standards, appropriate use of technology to enable information-sharing and a robust approach to data ethics, with due regard to privacy protection and the potential for analytical bias. The framework should be accompanied with transparent performance reporting and accountability.

This paper is primarily intended to provide a basis for further engagement with policymakers, supervisors and both private sector and public sector leaders involved attempting to respond to economic crime threats. We hope this paper is a useful reference document and can support consideration, feedback and the sharing of insight in relation to the enabling themes and contributing factors.

Endnotes

[1] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version
[2] https://www.FATF-gafi.org/media/FATF/documents/recommendations/Private-Sector-Information-Sharing.pdf
[3] See FATF (2018), Professional Money Laundering, FATF, Paris, France
[4] FATF, 'Professional Money Laundering', 2018. <http://www.FATF-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html>
[5] Monetary Authority of Singapore (1 October 2021) CONSULTATION PAPER ON FI-FI INFORMATION SHARING PLATFORM FOR AML/CFT
[6] See Maxwell, N (2020) Future of Financial Intelligence Sharing (FFIS) research programme 'Five years of growth in public–private financial information-sharing partnerships to tackle crime'.
[7] https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html?hf=10&b=0&s=desc(fatf_releasedate)
[8] https://www.fatf-gafi.org/media/fatf/documents/Stocktake-Datapooling-Collaborative-Analytics.pdf
[9] https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/stocktake-data-pooling-collaborative-analytics-data-protection-handout.pdf
[10] https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html?hf=10&b=0&s=desc(fatf_releasedate)
[11] https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/stocktake-data-pooling-collaborative-analytics-data-protection-handout.pdf
[12] Maxwell, N (2020) Future of Financial Intelligence Sharing (FFIS) research programme 'Five years of growth in public–private financial information-sharing partnerships to tackle crime'.
[13] As described in Maxwell, N (2019) 'Expanding the capability of financial information-sharing partnerships' RUSI Occasional Paper - https://www.future-fis.com/thought-leadership-in-partnership-development.html
[14] https://home.kpmg/au/en/home/insights/2020/12/battling-economic-crime.html
[15] https://rusi.org/sites/default/files/the_silent_threat_web_version.pdf
[16] Tiggey May and Bina Bhardwa, Organised Crime Groups Involved in Fraud (London: Palgrave Macmillan, 2018), p. 23.
[17] May and Bhardwa, Organised Crime Groups Involved in Fraud, p. 61.
[18] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
[19] https://www.fincen.gov/sites/default/files/shared/sar_tti_23.pdf
[20] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
[21] https://www.fincen.gov/sites/default/files/shared/314bparticipationinfo.pdf
[22] https://www.fincen.gov/sites/default/files/shared/314bInfographic.pdf
[23] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
[24] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1018157/E02671867_CP_520_Treasury_Minute_Accessible.pdf
[25] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime
[26] https://www2.deloitte.com/uk/en/blog/economic-crime/2021/bringing-economic-crime-to-justice.html
[27] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime
[28]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf
[29] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version
[30] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version
[31]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf
[32] UK Home Office, Economic Crime Engagement Exercise Paper – November 2021 (Unpublished)
[33] https://www.legislation.gov.uk/uksi/2014/1608/made
[34] https://gdprhub.eu/Article_6_GDPR
[35] Synectics Solutions also in deployment in other jurisdictions
[36] This survey focuses on the UK FISS service, but UK Finance also host a range of collaborative forums relevant to fraud information sharing between members; including the Best Practice Standards (BPS) and Fraud Indemnities services. The BPS Background - UK Finance worked with the industry to develop a voluntary set of standards for Sending and Receiving Firms to follow when processing a claim of an APP scam. The standards removed the barriers for first generation information sharing, increasing the number and speed at which mule accounts are identified and the value of fraud funds frozen and repatriated. In September 2020, UK Finance launched a dedicated secure information sharing messaging platform to support BPS standards. On average 4,200 cases have been reported per month. UK Finance stated in this research process that the BPS platform currently hosts over 85% of the market. Fraud Indemnities Background – This is a case management platform which was launched in March 2021. The platform enables firms to efficiently raise, track and respond to unauthorised fraud cases. On average 1,500 cases are reported per month. Since the BPS functionality launched in September 2020, a total of £21,438,019 of has been frozen and repatriated back victims, whilst in the unauthorised space, since the indemnities functionality launched in March 2021, £4,972,387 has been frozen and repatriated.
[37] While the Articles of Association of Cifas permit information sharing on fraud and money laundering, in practice - at the time of this research - money laundering and terrorist financing information is not currently shared through Cifas.
[38] https://gdprhub.eu/Article_6_GDPR
[39] https://www.cifas.org.uk/insight/reports-trends/fraudscape-2021
[40] https://www.fraudscape.co.uk/
[41] https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf
[42] Described in detail in Maxwell, N (2020) Future of Financial Intelligence Sharing (FFIS) research programme 'Five years of growth in public–private financial information-sharing partnerships to tackle crime'
[43] https://www.cityoflondon.police.uk/police-forces/city-of-london-police/areas/city-of-london/about-us/about-us/ifed/
[44] For more details on privacy preserving analysis relies on 'privacy enhancing technologies', or PETs, and the growth of this specialist cryptographical capability in the financial crime space, see Maxwell, N (2020) 'Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime' Future of Financial Intelligence Sharing (FFIS) research programme. Version 1.3
[45] In the sense that payments data is already pooled
[46] For a more detailed description of security of data in use and the role of privacy enhancing technology in financial crime use-cases – please see https://www.future-fis.com/the-pet-project.html
[47] However, in this case the platform may still provide strategic analysis and support member discussion on certain threats.
[48] COSMIC will initially focus on the following key risks: abuse of shell companies, trade-based money laundering and proliferation financing.
[49]UK Finance Survey Submissions to the FFIS Programme, 22 September 2021 and 11 February 2022
[50]UK Finance Survey Submissions to the FFIS Programme, 22 September 2021 and 11 February 2022
[51] https://gdprhub.eu/Article_6_GDPR
[52] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen
[53] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen
[54] https://gdprhub.eu/Article_6_GDPR
[55] The specific list of covered crimes is found here in (c)(7) https://www.law.cornell.edu/uscode/text/18/1956

[56] https://www.jdsupra.com/legalnews/fincen-provides-a-section-314-b-3443385/
[57] https://www.jdsupra.com/legalnews/fincen-provides-a-section-314-b-3443385/
[58] Monetary Authority of Singapore (1 October 2021) CONSULTATION PAPER ON FI-FI INFORMATION SHARING PLATFORM FOR AML/CFT
[59] Monetary Authority of Singapore (1 October 2021) CONSULTATION PAPER ON FI-FI INFORMATION SHARING PLATFORM FOR AML/CFT
[60] https://www.cifas.org.uk/fraud-prevention-community/member-benefits/data/nfd/nfd-principles
[61] https://www.law.cornell.edu/cfr/text/31/1010.540
[62] https://gdpr-info.eu/issues/fines-penalties/#:~:text=For%20especially%20severe%20violations%2C%20listed,fiscal%20year%2C%20whichever%20is%20higher.
[63] https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering
[64] Salv submission to FFIS research programme on 1 February 2022.
[65] https://www.coe.int/en/web/cybercrime/the-budapest-convention
[66] https://www.eba.europa.eu/eba-alerts-detrimental-impact-unwarranted-de-risking-and-ineffective-management-money-laundering-and
[67] https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering
[68] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022
[69] https://www.gov.uk/government/publications/economic-crime-strategic-board-minutes-and-agenda-17-february-2021/economic-crime-strategic-board-17-february-2021-agenda-and-minutes
[70] UK NCA, 'National Economic Crime Centre Launched', press release, October 2018<http://nationalcrimeagency.gov.uk/news/1501-national-economic-crime-centre-launched>, ; UK NCA, 'National Economic Crime Centre announced', press release, 11 December 2017; NCA presentation to the FFIS dialogue roundtable, 12 October 2018.
[71] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen
[72] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen
[73] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/01/onderzoek-informatie-uitwisseling
[74] https://www.nautadutilh.com/en/information-centre/news/new-plan-to-combat-money-laundering
[75] https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html?hf=10&b=0&s=desc(fatf_releasedate)