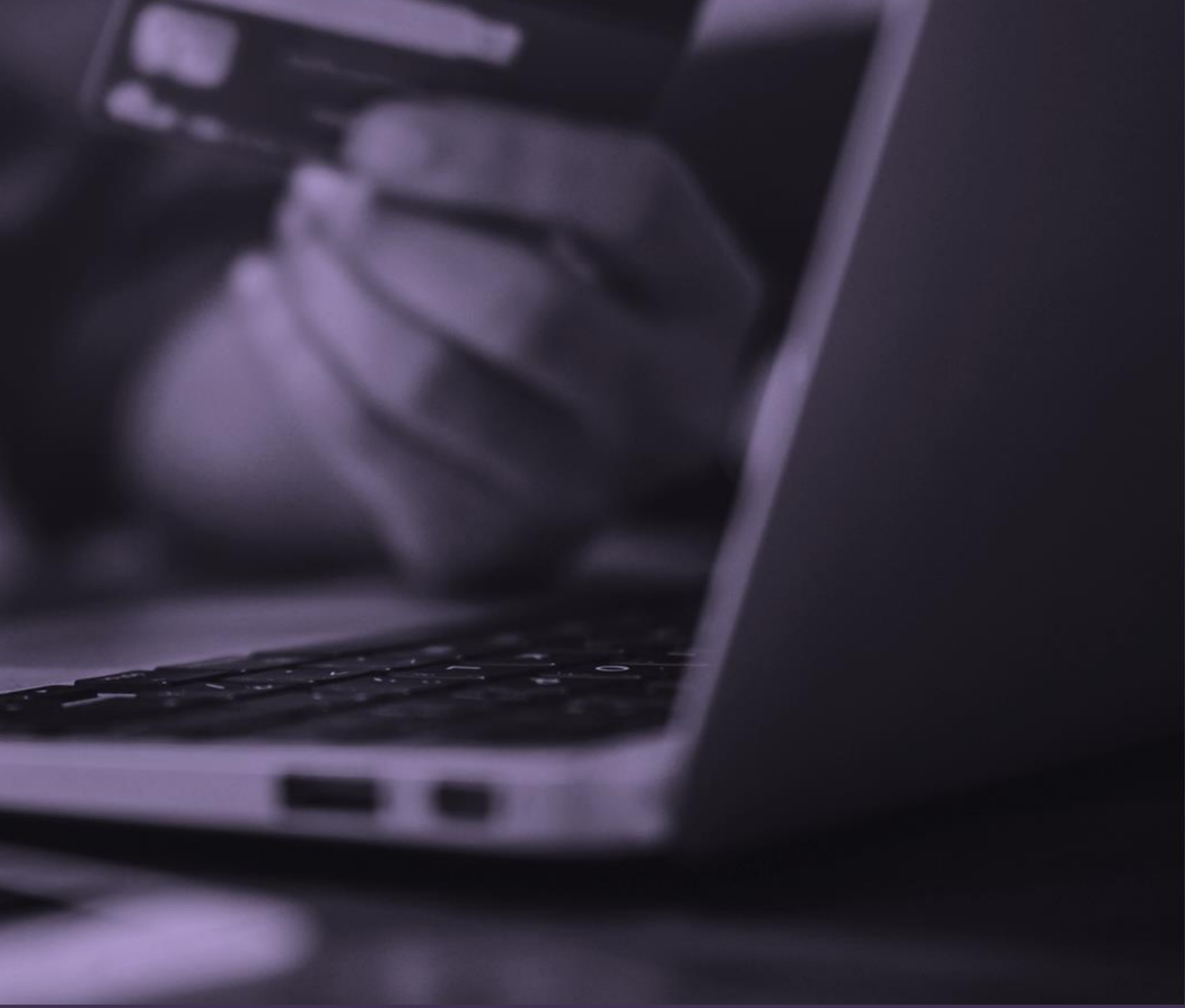


Future of Financial Intelligence Sharing (FFIS)

Payment Systems Policy Discussion Series

Paper 1:
‘The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk’

January 2024

FFIS Policy Discussion Paper

The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk

January 2024

About

This Discussion Paper is part of a series intended to support policy-makers and other interested parties to consider the role of payments infrastructure in enhancing the detection of economic crime. This paper has been prepared by the Future of Financial Intelligence Sharing (FFIS) research programme as part of our mission to conduct independent research into the role of public-private and private-to-private financial information-sharing in detecting, preventing and disrupting crime. The FFIS programme is a research partnership within the 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 Discussion Paper and our broader research programme. This research project would not be possible without grant funding support from:

- HSBC
- PayTM
- Deloitte LLP
- Verafin
- Synectics Solutions

We are very grateful to all those who have participated in research interviews, research workshops and broader conferences associated to this study.

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 for detecting and disrupting of economic crime.

All information in this paper was believed to be correct by the author as of 4 January 2024. 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.

Author: Nick Maxwell

Reference citation: Maxwell, N (2024). Payment Systems Policy Discussion Series, "Paper 1: The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk". Future of Financial Intelligence Sharing (FFIS) research programme.

Contents

Explaining the case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk

Executive Summary

This first discussion paper in the FFIS *Payment Systems Policy Discussion Series* is intended to facilitate greater dialogue and understanding about opportunities and challenges to draw more value from national payments infrastructure to identify and disrupt economic crime.

This paper forms one of a series of four discussion papers, comprising:

- Part 1: The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk;
- Part 2: The case for the G20 cross-border payments reform 'Roadmap' to embed economic crime security by design;
- Part 3: The case for the Financial Action Task Force to update and renew the concept of payment transparency; and
- Part 4: The case for international coordination in the use of ISO 20022 for economic crime detection purposes.

In Part 1 of this series, we focus on the case for policy-makers, relevant authorities and payment system operators to maximise the extent to which national payment infrastructure is utilised to identify economic crime risk, through open APIs, in a vendor-neutral manner and subject to governance controls. We further recommend that national payment reform processes and economic crime security considerations, encompassing both fraud and financial crime, are coordinated on an ongoing basis.

The historic approach within the anti-money laundering and counter terrorist financing (AML/CTF) regime, which relies on individual financial institutions and other regulated entities to look at their view of a customers' payment data to determine risk in isolation, has failed to deliver meaningful outcomes. The policy case to shift from this approach and support collaborative analysis in detecting economic crime is compelling.

The Financial Action Task Force, the Bank for International Settlements and various studies by FFIS and other parties have identified the significant value of multi-party collaborative analysis of payment flows to detect economic crime.

A major FFIS survey in 2022 identified that, by engaging in collaborative analytics, private-sector entities were able to identify 5 times the number of money laundering ‘subjects of interest’ previously unknown to law enforcement and public authorities were able to achieve an 85% time saving for complex network analysis in money laundering cases.

In July 2022, the FATF recommended that countries support collaborative analytics to detect risk by developing bespoke legislation to allow the private sector to share risk information, by encouraging innovation and pilot projects for collaborative analytics and by considering whether the public sector can establish relevant data infrastructure for collaborative analytics to take place.

This FFIS discussion paper highlights the substantial data and operational efficiency advantage of utilising national payments infrastructure for economic crime related analysis. While the FATF have previously recommended that new private sector collaboration initiatives and new data infrastructure be considered to enable such initiatives, our study identifies that there is considerable value in utilising *existing* central payments infrastructure for the same objectives.

Part of the value inherent in utilising payments infrastructure is in the cost-saving and project management efficiencies of using existing data, operational and legal frameworks. However, arguably, the key advantage is the increased scale of data available at the level of central payments infrastructure. This data superiority can support more effective and more precise risk modelling, enables a more comprehensive ability to identify organised crime and money laundering networks and can better facilitate the tracing and recovery of stolen funds.

In this study we find that, when observing the two approaches in one country, an analytical platform at the level of central payments infrastructure has a 500-fold data advantage over a comparable collaborative analytics project that relied on establishing new data infrastructure for combining transaction data.

Following from the UK example of the ‘New Payments Architecture’ initiative, national payment infrastructure can be made accessible by a range of accredited and authorised third-parties to run different types of economic crime related analysis. In this paper, we argue that a vendor-neutral open API framework can be achieved for central payments infrastructure data and a ‘democratisation’ process can take place with regard to what is some of the most important national data relevant to identifying financial crime and fraud. This openness can improve innovation, diversity of use-cases, overall effectiveness and encourage inter-operability between systems for identifying economic crime risk.

A key dependency for achieving these reforms is the ability to bridge the gap between payments, AML/CTF, sanctions and fraud prevention policy and practitioner communities.

Payments infrastructure is, perhaps, an obvious focus point for economic crime related analysis. It is also an under-utilised capacity. Arguably, this is because of the challenges involved in achieving coordination between payments reform and economic crime related policy-making stakeholders.

This paper aims to support that coordination process and promote dialogue between the relevant communities to better unleash the potential of payments infrastructure to protect society from economic crimes.

Methodology

This discussion paper series is the product of:

- Open-source research/literature review of relevant materials;
- Policy analysis of research material related to the FFIS 2022 survey process covering 15 private-to-private sharing platforms around the world;
- Critical analysis of discussion at four FFIS project events and three major inter-governmental multi-stakeholder conferences which convened international experts from public and private sectors relevant to the field;[1]
- Additional interviews with key stakeholders;
- Feedback and peer-review on draft versions of the study.

This paper extends on recent landmark publications at the inter-governmental level related to collaborative analytics to tackle economic crime and the role of payments infrastructure in supporting such analysis.

Specifically, this paper builds from:

1) The Financial Action Task Force '*Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing'* best practices paper;[2]
2) The Bank for International Settlements *'Project Aurora'*[3], which established quantitative measures for the value of economic crime analysis taking place at the level of national and cross-border payments infrastructure and the utility/privacy considerations of use of privacy enhancing technology; and
3) The Europol Financial Intelligence Public Private Partnership (EFIPPP)[4] exploration of the barriers to fraud-risk messaging through payments infrastructure which took place through the Innovation Working Group of EFIPPP from September 2022 to April 2023.

The primary research cut-off period was 4 January 2024 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'**[5], which covers activity 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; and
- the recovery of criminal and terrorist assets is also in scope.

In terms of sectoral coverage, the paper is primarily concerned with payment service providers and payment system operators, including central payment market infrastructure systems for settlement and clearing (at the national and international level).

There is no universally agreed definition of terms used in the context of payment systems and central payments infrastructure. In this paper we adopt the following definitions which have been proposed in a comparative analysis paper compiled for the UK's Payment Systems Regulator:[6]

- **Payments system** includes interbank financial market infrastructure whose primary function is to facilitate the exchange of electronic payments for goods and services.
- **Payment system stakeholders** includes the payment scheme rule makers and managers, the technical infrastructure operators and the regulators that together ensure the successful operation of the clearing and settlement of electronic payments.
- **Payment system operator** is a company that operates one or more payment schemes.
- **Central payment infrastructure** is the hardware, software, connections and operations that support the clearing and/or settlement of a payment or funds transfer request after it has been initiated.

This study seeks to draw from experience in two main policy domains of economic crime – anti-money laundering and fraud prevention.

The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk

Key insights:

- Effective detection of economic crime risk requires analysis of connected payments data between multiple financial institutions and other payment service providers.
- Collaborative multi-party detection systems in the private sector have demonstrated numerous advantages (including increased detection of risk and enhanced efficiency of processes) and are recommended by the Financial Action Task Force in the *'Partnering Against Financial Crime'* best practices paper.[7]
- The latest data from U.S. case studies indicates that collaborative analytics can provide substantial benefits in reducing false positives and lowering the propensity of regulated entities to file low-quality 'defensive' reporting. Such results can enhance the quality of reporting to Financial Intelligence Units, enable more accurate models of risk to be trained and better protect citizens' privacy rights and innocent parties within the AML/CTF regime.
- Utilising payment infrastructure as part of collaborative economic crime detection systems can achieve greater scale, improve effectiveness and reduce 'start-up' and operational costs compared to building new data infrastructure to pool transactions.
- Establishing access to national payment infrastructure data in an open API framework, under the appropriate governance framework, can enable authorised third-parties specialising in economic crime detection to drive innovation, diversify use-cases and maximise the value and opportunity of payments data to address national economic crime threats.
- With greater policy coordination between payments reform and economic crime policy stakeholders, economic crime detection systems can be integrated into payments infrastructure and allow for more effective and more targeted outcomes.
- Building from early-stage innovation, there is now an opportunity for policy makers to consider how to maximise the potential of payments infrastructure to support detection of economic crime risk. This paper proposes key policy considerations to across five principles: leadership; legal clarity; governance and regulation; technology; and evolution.

Key statistics in this section:

- 5x more subjects of interest to money laundering criminal investigations identified through collaborative analytics in the U.S.
- 85% time-saving achieved by public agencies involved in investigating complex money laundering networks in The Netherlands when interacting with a private-sector collaborative analytics platform, compared to bi-lateral engagement with individual financial institutions.
- 60% reduction in false positives achieved through collaborative analytics in the U.S. and a 50% reduction in false positives achieved through collaborative analytics in the UK.
- 20% more fraud identified in a real-world data proof-of-concept in the UK when using enhanced data-sharing through the payment system.
- 2x to 3x more embedded money laundering networks identified through analysis at the level of central payments infrastructure, compared to what could be discovered by individual financial institutions conducting analysis on their own data in silos, in a synthetic-data international proof-of-concept run by the Bank for International Settlements.
- 500x more account data available for analysis in the UK at the level of central payments infrastructure, compared to an AML collaboration initiative which pooled transaction data in new data infrastructure over the same period.

Key recommendation:

- National (or EU) policy-makers, relevant authorities and payment system operators should seek to maximise the extent to which payment infrastructure is utilised to identify economic crime risk, through open APIs, in a vendor-neutral manner and subject to appropriate governance controls; including a holistic approach to fraud, AML/CTF and sanctions threats.

  ____

  Key dependency for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk: Coordination and strategic vision at the policy-making level which encompasses public sector (and, ideally, private and third sector involvement) from across payments, AML/CTF, sanctions and fraud prevention policy and practitioner communities.

Explaining the case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk

Why analysis of connected payments data is important for the detection of economic crime

Analysis of payments visible to an individual financial institution provides only a fragmented view of economic crime networks

Money laundering attempts are spread across multiple accounts and multiple institutions and, indeed, seek to move value quickly across different types of payment systems, different 'stores of value' and across borders.

In general, national frameworks for identifying money laundering have relied on placing regulatory obligations on individual private sector entities to examine their customer data to identify and report suspicious activity.

However, it is increasingly recognised that transaction analysis to identify money laundering risk at the level of individual regulated entities has a low efficacy due to limited visibility of the target activity.[8]

The more that transaction data can be analysed collectively or collaboratively, connected between the relevant financial institutions, the greater the efficacy will be of analysis to uncover economic crime networks and activity.

As the 2023 Deloitte Payments Architecture White Paper puts the challenge:

> *"Ultimately, the current AML system is not fit for purpose. Criminals are able to launder money through complex, multi-institutional and multi-jurisdictional schemes. Detecting these schemes requires collaboration and coordination between private and public sector stakeholders. Removing silos between data sets is fundamental but, currently, sharing information between organisations is challenging."*[9]

Collaborative analysis of payments data provides significant advantages to detect economic crime

Since the 2020s, the FATF[10] have highlighted that multi-institutional data-sharing and collaborative analytics are critical for effective AML/CTF efforts.[11] More broadly, digital transformation has been a strategic priority of the FATF for enhancing AML/CTF effectiveness, including considering public-private information sharing, private-to-private sector information sharing, privacy enhancing technology and relevant data protection policy considerations.[12]

Box 1: Summary of the FATF best practice guidelines in "Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing" (July 2022).[13]

Analysing case studies of private-to-private sharing of information relevant to AML/CTF obligations, the FATF noted:

"Based on various discussion the FATF has had with both the private and public sectors, it is increasingly difficult for a single private sector entity to identify suspicious transactions in complex schemes designed to avoid detection. The FATF and other stakeholders have reported on intricate ML/TF/PF schemes that involve complex legal arrangements and transaction patterns that are difficult or impossible to detect without information from counterparty banks or other banks providing services to the same customer or its associates. Furthermore, as the number of transactions grows, it may be increasingly complicated for transaction monitoring systems to pinpoint suspicious activity. Without the ability to access and process additional information among private sector entities, there is a risk that these systems may be capturing transactions which are not relevant, and reporting false positives as a result."[14]

FATF recommend that the public sector should:

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

Private sector participants are encouraged to develop collaboration innovation including (through the application of privacy enhancing technologies and strengthening data interoperability). Private sector stakeholders are also called on to pursue data-protection by design and prevent excessive or unwarranted de-risking through collaboration.

In effect, this FFIS discussion paper explores the relevance of these FATF recommendations to payments infrastructure.

In 2022, FFIS published a survey and policy discussion paper *'Lessons in Private-to-private Financial Information Sharing to Detect and Disrupt Crime'*, which covered 15 different platforms for private-to-private economic crime related collaboration. The survey reported on the outputs and outcomes, quantitative and qualitative, that were being observed by collaborative multi-party economic crime analysis platforms. In terms of the value to public sector agencies that utilise the end-product of such platforms, the survey highlighted a 5 times increase in private-sector entities being able to identify subjects of interest previously unknown to law enforcement and an 85% time saving for public authorities by engaging a collaborative analytics platform, compared to engaging with the individual financial institutions bi-laterally.[15]

Private-to-private financial information sharing platforms typically have the following objectives:

- Improved detection of economic crime risk;
- Reduced duplication of processes and cost for pooled or shared activity; and
- Reduction in displacement of risk (between members of the platform).

Greater collaboration in economic crime related analysis typically increases the volume of relevant data for analysis and increases the visibility of potential economic crime networks. Greater volumes of data also enable machine learning techniques to identify economic crime risk with greater precision.

Private-to-private financial information-sharing partnerships can also support enhanced resolution on risk and reduce false-positives, which may reduce the propensity for financial institutions to deem a client as ‘suspicious’ when information from counterparties can provide explanations to resolve concerns or alerts.

Box 2: Case study on information sharing in the United States under section 314(b) of the PATRIOT Act through Verafin and the potential to reduce ‘defensive filing’.[16]

When considering the need for filings to be high quality and useful to law enforcement and, more fundamentally, to protect the privacy of innocent parties - an important metric for success is the reduction of false positives and, accordingly, a reduction in the propensity for ‘defensive’ or unnecessary regulatory filings.

Defensive filings may occur when there is some level of indicator of risk associated to a transaction or customer, and - in the absence of any other reason not to file a suspicious report - there is a perceived regulatory pressure to file the report of ‘suspicious’ activity. Regulatory pressure in the

AML/CTF system is focused on ensuring filings of suspicious activity are made to Financial Intelligence Units and there is no regulatory disincentive for over-filing.

Verafin, a Nasdaq company, provides a cloud-based software platform for financial crime management, including fraud detection, AML compliance, high-risk customer management and information sharing. Section 314(b) of the USA PATRIOT Act is the principal legal gateway for financial crime related information sharing between authorised entities.[17]

Verafin operates one of the largest 314(b) associations of financial institutions in the United States.

In terms of reducing defensive filing, in analysis of more than 56,000 case investigations between 2018-2022 where financial institutions and other entities utilised 314(b) collaboration tools in Verafin's platform, nearly 60% of those cases were resolved as 'not suspicious' after an act of communication or collaborative investigation.

This indicates that when Verafin members had an initial cause for concern relating to money laundering or suspicious activity and had initiated a communication or collaboration on the matter, they were able to resolve their concern when additional information was available from counterparties in 60% of cases.

In these cases, a member has closed their investigation without reaching the threshold of 'suspicion' and therefore a filing would likely not have been required to the government Financial Intelligence Unit on that individual or entity.

Reducing the level of defensive reporting improves the quality of reporting through to Financial Intelligence Units and plays an important role in safeguarding the privacy of citizens.

High-quality assessments of economic crime risk are also essential to instruct detection models and use them to identify further risk.

In the absence of such collaborative analytics or information sharing frameworks, these low-quality 'defensive' filings would likely be made to the Financial Intelligence Unit, and the internal detection systems of the financial institution would continue to identify and report on similar instances without being able to learn or adapt the detection model.

However, collaboration platforms can face significant challenges in developing and achieving scale.

The FFIS 2022 survey identified and quantified the impact of economic crime-related collaboration, where multiple financial institutions can share data relevant to identifying risk. However, the study also noted several barriers and limitations associated to collaborative analytical platforms that rely on new data infrastructure for pooling transaction data.

These include:

- Despite explicit encouragement from FATF to establish the legal basis for private-private sharing for AML/CTF purposes, only small number of countries have established such a legal gateway.
- Typically, there are complex project management, operational, legal and regulatory issues to address when establishing new collaborative ventures between multiple regulated entities to combine transaction data.
- New collaborative analytics platforms can often face significant limitations in their membership size, the sectoral coverage and the diversity of payment types which are included in the platform.
- As a result of the limited membership and payments visibility, collaboration platforms have a corresponding restriction or limitation in being able to observe money laundering networks that span beyond the membership.
- In terms of tracing money laundering flows, platforms are not necessarily able to identify payment dispersals which leave their membership or payment framework and return to the network membership as a result of a process of money laundering.
- To date, economic crime collaboration initiatives are largely national, where they do exist, and unable to conduct cross-border analysis.

Given the complexity of establishing new data infrastructure for combining transactions between multiple parties, this paper argues that it is important for policy-makers to seek to leverage existing data architecture to achieve the vision of the FATF's *'Partnering in the Fight Against Financial Crime'* guidelines.

Central payments infrastructure is where transaction data is already collated

National and cross-border payments infrastructure for payment instruction, clearing and settlement benefit from substantially greater visibility of payment flows between financial institutions than do individual financial institutions. Insights into financial crime and fraud can be drawn from payments data and networks of payments, even if the data is limited to payment sender, beneficiary, amount and timestamp.

It is important to recognise that central payments infrastructure data, and the particular interest in this paper is real-time and faster payment rails, still has substantial limitations in that there are numerous types of payment which do not flow through such payment rails, including: payments within a financial institution; cash; credit card; digital wallet payments; and/or virtual asset service providers, for example. Payment rails will also not replace requirements for 'Know Your Customer' (KYC) data, which is principally held by the institutions with a direct relationship with a customer.

Despite these limitations, payments and settlement central infrastructure is a natural centralised data source for financial flows which can be used to understand networks of criminality stretching across multiple financial institutions. As a result, central payments infrastructure has clear advantages for analysing risk related to payment flows, though could not replace the KYC and behavioural insights available to individual financial institutions and other regulated entities.

Payments data analysis should be seen as having benefits to augment an understanding of economic crime risk, including to those parties who may have more detailed information on a subject of interest - such as bio-metric and telemetric data.

However, historically, the use of payments infrastructure for economic crime analysis has been limited

The FFIS 2022 survey noted that - apart from one example in the survey - payments infrastructure has not been used as a basis for money laundering analytics at the national level. The leading example of such analysis in the FFIS survey was the Mastercard Vocalink 'Trace' platform, which runs on the UK Faster Payments and UK Bacs payment rails and does not require additional pooling of transaction data beyond what is provided for the operation of the payments frameworks.

Outside of the UK, a number of national payment systems provide fraud alerting capabilities based on analysis of typologies of behaviour or anomalies or provide protections against fraudulent payments through ‘confirmation of payee’ checks at the level of central payments infrastructure. However, these capabilities generally fall short of the level of analysis which is demonstrated in the UK Vocalink platform to trace money laundering networks and enable investigations and recovery of funds.[18]

The impact of collaborative analytics to detect economic crime using central payments infrastructure

Vocalink financial crime behavioural models are developed from a data-driven approach, using large-scale payments data from multiple financial institutions and providing intelligence beyond an individual financial institution’s partial view. [19]

Analysing data from 12 participating financial institutions, two payments schemes and Financial Fraud Action UK (FFA UK), Vocalink successfully overlayed analytical techniques to highlight the existence and scale of suspect mule accounts operating within the banking network and map the movement of funds through the UK payments systems.

Within a few weeks of going live in Q4 2018, the following results were recorded[20]:

- 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.

The initiative observed improved detection rates; faster speed of response; enhanced prevention of ‘loss to fraud’; recovery of funds; reduced stolen funds exiting the banking system; and reductions in observed money laundering attempts targetting participating institutions’ accounts to extract funds.

By June 2022, the Vocalink algorithms had analysed 20 billion transactions and were trained on 700 million money laundering data points relevant to 50,000 identified money laundering typologies or ‘motifs’.[21]

With regard to consumer fraud risk (retail payments fraud), Vocalink demonstrated that false positive levels could be reduced by 50% with only an 8% reduction in detection of networks.[22]

A UK 'Enhanced Fraud Data' proof-of-concept on 6-months of historic transaction data, utilising enhanced data sharing through the payment system, identified that UK banks could have prevented, on average, 20% more fraud compared to what was identified without the additional data.[23]

The advantage of utilising central payments infrastructure for economic crime detection

In 2023, the Bank for International Settlements published the results of *'Project Aurora'*, a major technical proof-of-concept examining the potential of national and cross border payments infrastructure to identify money laundering networks. Project Aurora concluded that, compared to what could be discovered by individual financial institutions conducting analysis on their own data in silos in rule-based scenarios, analysis at the level of payments infrastructure could be expected to identify 2x to 3x more embedded money laundering networks.[24] The Bank for International Settlements project concluded that "analysis of payments data is highly valuable for AML … [providing] greater visibility and improved detection of suspicious networks and illicit payment flows across financial institutions and borders."[25]

The key advantages of running economic crime analytics at the level of central payments infrastructure revolve around (1) the greater volumes of data available and (2) the operational and legal efficiency benefits of working through a system which is already established.

With access to broad national-level payment data, the accuracy of detection models expands significantly compared to models trained on individual financial institutions.

Across two years of proof-of-concept data, Mastercard Vocalink Trace connected nearly 100 million accounts across 12 financial institutions, detailing over 357 million individual payment relationships.[26] This compares very favourably to a UK collaboration initiative for AML transaction monitoring, operating at the same period, which relied on developing new data infrastructure for pooling transaction data. The UK *'Tri-bank initiative'*, which involved 3 UK banks, was limited to analysing historic data on small and medium sized corporate client data as a proof of concept in 2018-2020. Within this initiative, there were approximately 200,000 accounts that had a common link within the network and could be analysed for money laundering risk.[27]

Comparing the two initiatives: analysis of data at the level of central payment infrastructure was able to cover 500 times the number of accounts than the Tri-Bank initiative. The UK Vocalink example also was able to analyse a broader array of customer types across more financial institutions.

In France, the STET national switch creates behavioural profiles for fraud prevention based on 255 million cards and 2.1 million merchants accounting for 6.7 billion card transactions annually.[28] This is 37.5 times more transactions than Mastercard Vocalink reviewed in the proof-of-concept stage, per year.

The advantage in scale when conducting analysis through payments infrastructure:

500x

The data advantage for account analysis at the level of central payments infrastructure compared to a transaction monitoring collaboration initiative which pooled transaction data in new infrastructure in the same period and same country.

Table 1: Data availability to apply and train anomaly detection and economic crime models in the UK:[29]

Initiative	Type of collaboration	Transaction data analysed	% increase
Tri-bank UK	New data infrastructure	200,000 accounts with connected transaction data from 3 financial institutions	An average three-fold increase compared to what an individual financial institution would observe in relation to similar data fields.
Mastercard Vocalink (UK)	Existing national faster payments and Bacs data, but with limited membership	100 million accounts across 12 financial institutions and analysing over 357 million individual payment relationships.	500 times the number of accounts compared to Tri-bank UK
STET national switch (France)	Existing national card payments data	6.7 billion card transactions analysed annually	37.5 times more transactions than Mastercard Vocalink, per year at proof-of-concept stage

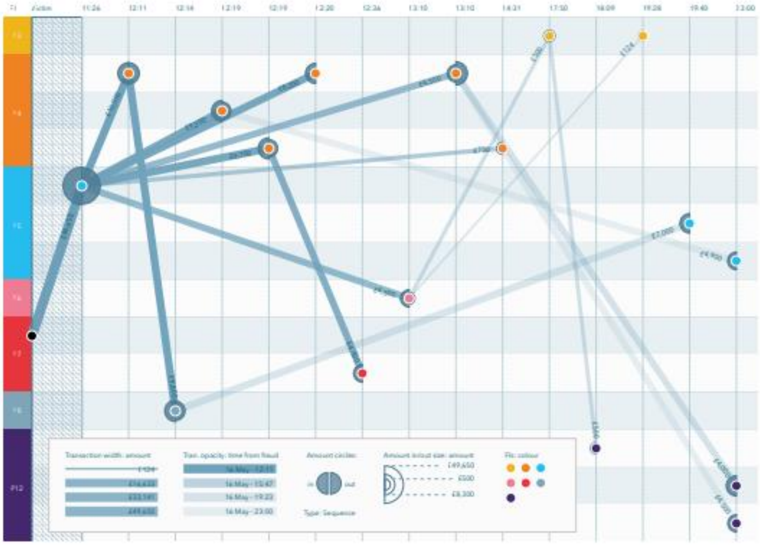
Economic crime detection use-cases for data at the level of central payments infrastructure:

There are a significant number of economic crime detection use-cases that could be enhanced through a connection to central payments infrastructure data. Different use-cases may require different types of data to be shared and require individual attention in terms of potential data protection implications. Use-cases which do not require sharing of personal data may be more suitable in the absence of specific enabling legislation to allow for private-to-private information sharing of personal data for economic crime detection or prevention purposes.[30]

Potential use-cases for payment rail data include:

- **Track, trace and alert capability:**
  Payment systems can allow participants in a payment network to benefit from a collaborative ability to trace the dispersal of funds from an identified high-risk account or economic crime incident, either from an identified exit or entry point to a payment system. This capability can support intelligence and investigative objectives and counterparties can be alerted to their exposure to risk of an identified money laundering network. Such tracing capabilities are essential in efforts to identify and restrain stolen funds, for example.

Figure 1. Rapid payment dispersal networks demonstrated by Mastercard Vocalink on UK faster payments data, covering multiple institutions in a short time frame.[31]



Box 3: The European Payments Council (EPC) recommendations on tracing capabilities[32]

In the *'2023 Payment Threats and Fraud Trends Report',* the European Payments Council (EPC) recommended:

> *"Regulators and PSPs should consider having mechanisms in place to react and stop supporting service practices or to put related transactions on hold, until further investigated, if transaction patterns indicate [money laundering] mule activity."*
>
> The report identified that *"Whereas the first mule level has a short lifetime, subsequent mule-levels may re-use accounts over a longer period if they can stay undetected."* And so:
>
> *"To detect complex mule and money laundering schemes… [if] PSPs [can] cooperate and pool their payment data (in a secure and lawful way), it may be possible to use strong analysis tools and much more efficiently detect mule accounts and money laundering rings."*
>
> The European Payments Council added, *"to be effective in the long run, such cooperation must be cross-border and will become even more important in view of instant payments, which are expected to gradually become the new normal."*

- **Typology and model deployment on connected transaction data:**
  Regardless of the development of a payment trace and alert capability, payment systems can allow for deployment of detection models, based on behavioural typologies of economic crime, on connected payments data. This capability can illuminate risk that is not observed by any individual participant and can alert participants who are exposed to behaviour that matches the risk model. Once a specific typology has been developed, the wider prevalence of the typology across the network can be determined. Utilising machine learning, models can be further developed by 'training' on connected data to identify additional risk.

Box 4. Machine learning model insights developed through consortium-level transaction monitoring[33]

Large volumes of data can enhance machine learning processes and enable more precise risk identification.

In the U.S., Verafin's machine learning analytics leverage consortium-level data from its client base, comprising:

- 2,500 financial institutions that utilise its transaction monitoring, analytics and investigation platform for fraud detection and anti-money laundering; and
- Payments data covering over 575 million counterparties; and

- Monitoring of over a billion transactions per week and an underlying value of USD 4.5 trillion in collective assets in members' customer accounts.

By leveraging this data - combining standardised alert data and investigative insights from individual members, running network-level analysis and augmenting additional third-party data sources - Verafin can profile counterparties of transactions and payments, including accounts and entities outside its network. Insights into lower and higher-risk counterparties from this consortium data are incorporated into Verafin's collaborative analytics in the form of risk scores.

In a proof-of-concept project with a large U.S. bank, Verafin delivered a 25% false positive alert reduction and a 250% improvement in detection of wire fraud (by value), when the results of Verafin's machine learning models, trained with wider consortium data, were compared with the financial institution's individual performance.

- **Communication of risk scores:**

  Payment infrastructure systems can provide members of a payment network with a capability to share assessments of risk scores on particular accounts in order to support further analysis for economic crime purposes. These alerts may be directly relevant to other counterparties exposed to that specific risk or they may serve to instruct network-level risk models. More widely, payment systems could be used to enable members to send messages and responses to one another related to economic crime risk questions on specific payments. As identified in the previous section, such communication can both enhance clarity on risk and, also, resolve concerns about economic crime.

Public sector use-cases:

Payment infrastructure systems could also be engaged by public sector authorities and enforcement agencies for economic crime detection and intelligence purposes.

In a 2023 White Paper, Deloitte proposes the following use-cases for anti-money laundering public-private partnerships to leverage payments infrastructure data:[34]

- **Supplemental intelligence gathering following a suspicious activity report or other lead:** Law enforcement or financial intelligence units could draw from central payments infrastructure data to illuminate a network of payments surrounding an account identified by a recent suspicious activity report or to identify close associates of a suspect.

- **Strategic assessment of impact of law enforcement or regulatory interventions:** Law enforcement agencies, financial intelligence units or regulatory authorities could utilise payments infrastructure data to help assess the impact of a particular intervention on an organised crime group or broader crackdown on a typology related to economic crime.
- **Public sector monitoring for specific money laundering typologies:** Law enforcement, financial intelligence units or regulatory authorities could utilise payments infrastructure data monitor for a high-priority money laundering typology that would not necessarily be visible to individual regulated entities.

An open-vendor approach to utilising national payments data

The use-cases above is intended to be indicative and is not exhaustive.

A key point for policy-makers to note is that the nature and extent of economic crime detection use-cases does not need to rest with the payment system operator themselves or be restricted to one organisation alone.

Policy-makers can create an open-API environment for payments data to be accessed by (multiple) authorised third-parties to allow market innovation to drive use-case development, under an appropriate governance framework.

As a major development in the UK's regulatory approach underway at the time of this study, Pay.UK are developing the UK's New Payments Architecture (NPA) which will support payment providers to access instant payments. Pay.UK is a non-profit organisation supervised by the Bank of England and regulated by the Payment Systems Regulator and operates most of the payment infrastructures in the UK[35] alongside the Bank of England's wholesale operations, CHAPS, and the real-time gross settlement (RTGS) payment system.

As a coordinated strategy covering 2021-2026, Pay.UK set out to support more effective fraud detection and better data-sharing within the NPA.[36] Pay.UK state in their strategy that "effective fraud prevention is essential for delivering world-class payment journeys. In our position at the centre of interbank payments, we recognise the crucial role we must play in the fight against fraud."[37]

Critically, Pay.UK intend to operate the NPA as a vendor-neutral platform. As such, Pay.UK will set rules, standards and governance to ensure wider access to payments data to be able to support economic crime related services and outcomes.[38] The open nature of NPA raises the possibility for multiple vendors offering a suite of different analytical services to make use of UK payments data, subject to governance controls.

In the 2023 Payments Architecture White Paper, Deloitte commented "if the NPA can act as an open environment which actively encourages different third parties to leverage its underlying data, it could prompt the release of a range of innovative services which financial institutions and law enforcement agencies might not have had the capacity or capability to architect themselves."[39]

As a comparable initiative to the Pay.UK NPA, though with a more limited capability focused on anomaly detection, the EBA CLEARING pan-European Fraud Pattern and Anomaly Detection (FPAD) functionality is intended to include a developer portal and sandbox to support users in the development and testing of FPAD's application programming interfaces (APIs).

This paper recommends that all countries seek to draw from these examples to allow private sector and third sector analytics to run on payments infrastructure data, particularly in national faster payment rails. Such an approach can empower private sector innovation to utilise the data (through a robust data governance framework) to develop capabilities that address economic crime threats facing a country.

The growth and limitations of current use of central payments infrastructure to detect economic crime

Growth in awareness and practice:

Inter-governmental authorities are increasingly recognising the potential of central payments infrastructure to detect economic crime and have encouraged national innovation in this regard.

The Bank for International Settlements Committee on Payments and Market Infrastructures (CPMI) have stated that:

> *"Operators of payment systems or messaging networks could work together with their participants, and other stakeholders, to evaluate what types of information and tools could effectively support the prevention and detection of wholesale payment fraud at the endpoints. These might include (i) participant-defined payment limits (eg payments will be processed only when they are addressed to a known correspondent within business hours and amount limits); (ii) payment screening against self-determined parameters; (iii) detection of unusual or*

> *uncharacteristic payment patterns (eg in terms of timing, value, volume or location); and (iv) frequent and timely (intraday) reconciliations."*[40]

The Bank for International Settlements set out in 'Project Aurora':

> *"Technology and collaboration could support financial institutions, central banks, supervisory and other public authorities to address AML challenges through collaborative analytics and learning … Such initiatives could leverage payment system-level data and public-private collaborative approaches to analyse privacy protected data to reveal suspicious networks and activities that may not be detected by financial institutions acting in isolation."*[41]

Several countries have explored some role for central payments infrastructure in economic crime detection; however, it should be noted that these initiatives are almost exclusively focused on fraud prevention rather than analytics covering broader financial crime types.

Box 5. International examples of economic crime-related analytics in payments infrastructure.[42]

USA: The U.S. Federal Reserve announced that the FedNow Instant Payment Service (with initial launch in July 2023) would include analytical tools to assist participating financial institutions in detecting fraud risk, including[43]:

- The ability for a financial institution to establish risk-based transaction value limits;
- The ability to specify certain conditions under which transactions would be rejected, such as by account number (a "negative list");
- Message signing, which will validate that the message contents have not been altered or modified; and
- Reporting features and functionality, including reports on the number of payment messages that were rejected based on a participating financial institution's settings.

The Federal Reserve is reportedly exploring *"other features that could be made available as part of future releases to aid participants in managing fraud risk, including, for example, value limits that could be tailored to certain uses, aggregate value or volume limits for specific periods (for example, per business day), and/or centralized monitoring performed by the FedNow Service such as functionality that leverages advanced statistical methods and historical patterns to identify potentially fraudulent payments."*[44]

Europe/SEPA: EBA CLEARING is a provider of pan-European payment infrastructure solutions, owned by 48 of the major banks operating in Europe and based on a country-neutral governance model.[45] In September 2023, EBA CLEARING announced an analytical pilot for pan-European Fraud Pattern and Anomaly Detection (FPAD) functionality, involving nine banks from six countries within the STEP2 and RT1 European payment systems.[46] In addition to an IBAN/name check, FPAD is intended to provide participants in the network with insights on patterns and anomalies from a central infrastructure level perspective, with anomalies qualified by feedback from participants.[47]

France and Belgium: ‘STET’ is a bank-owned provider of pan-European payment infrastructure solutions. It processes over 22 billion transactions a year as one of the major European clearing and settlement systems. Within Single Euro Payments Area (SEPA) rules, STET operates the CORE platform, which clears low-value payments for consumers and corporate clients in France and Belgium. STET offers fraud scoring as a value-added service for all payment types it processes.

Nigeria: Nigeria Inter-Bank Settlement System Plc (NIBSS) was incorporated in 1993 and is owned by all licensed banks including the Central Bank of Nigeria (CBN). NIBSS has specific responsibility delegated from the CBN for the provision of anti-fraud solutions and related services.

South Africa: BankservAfrica is the official clearing house for electronic payments, appointed by the Payments Association of South Africa (PASA). BankservAfrica has reported aspirations to develop a transactional fraud mitigation system as well as an account verification service.

India: The Reserve Bank of India (RBI) has encouraged payment system operators in India to put in place robust fraud and risk monitoring systems. In response the national clearing house, the National Payments Corporation of India, has designed and implemented a real-time transaction monitoring tool for fraud detection and prevention and offers this free of charge to its participants.

South Korea: South Korea encourages a holistic approach to payments fraud prevention and resolution, where the South Korea regulator, the Financial Supervisory Service (FSS), plays a large role in payments fraud prevention and resolution.

Netherlands: Utilising empty ISO20022 fields, financial institutions in the Netherlands are reportedly sharing the internal fraud score from sending party to receiving party. This enables the receiving party to better judge borderline cases where the information it has may be insufficient to flag a transaction as fraudulent.

Current limitations in economic crime-related analysis at the level of central payments infrastructure:

The case studies set out above indicate the extent to which fraud-focused analytics are being considered by countries as enhancements to their central payments infrastructure. While a number of these initiatives are promising, many are still aspirational or are in very early stages.

For those that are operational, the capabilities generally fall short of network wide analytics to develop and exploit models of risk, covering both AML and fraud risk, or being able to trace dispersals of funds.

The UK Vocalink Mastercard platform has demonstrated a more ambitious deployment of payments-level analytics and the capability to trace stolen funds through the payments system. However, even in this relatively advanced model, a number of limitations in the approach and framework of operations have been observed[48], including:

- Membership was limited to 12 financial institutions;
- There is no public-private partnership engagement in the analytical potential of Vocalink, such as through the UK National Economic Crime Centre or the UK Joint Money Laundering Intelligence Taskforce, which restricts the full use of the data analysis for disruption initiatives; and
- The full array of analytical capabilities and its application against a broader array of economic crime threats appears to be under-exploited by virtue of the limited contractual mandate and permissions that Vocalink was created under by the participating financial institutions.

Maximising the opportunity of payments level infrastructure for economic crime detection at the national-level

As highlighted in the previous section, in recent years there has been a significant early-stage innovation in utilising central payments infrastructure for more effective economic crime detection in a number of countries.

There is now an opportunity for policy makers to draw from this practice and consider how to maximise this potential. Further, we recommend that national payment reform processes and economic crime security considerations, encompassing both fraud and financial crime, are coordinated on an ongoing basis.

Realising this opportunity will require greater levels of coordination between policy-makers with authority over payment system reform and those with responsibility in leading national responses to financial crime and fraud. Too often these domains of policy-making are fragmented and uncoordinated.

In the original principles-based guidance for the development of public-private partnerships to tackle economic crime, FFIS set out five major principles to help frame policy making to encourage the growth of such initiatives. Those principles are:

1. Leadership
2. Legal clarity
3. Governance and regulation
4. Technology
5. Adaptability and evolution

In the section below, we use the same principles to suggest a framework for how policy-makers (and payment system operators and their regulators) can consider supporting national payment infrastructure to provide a greater contribution to national efforts to tackle economic crime.

Principle 1: Leadership

A major challenge in policy-making related to unleashing the power of payments infrastructure to detect economic crime is the fragmentation of policy-making across: payments reform, fraud prevention policy making, the financial crime policy sphere (which is mostly associated to the AML/CTF regulatory regime) and the financial sanctions regime.

Through the course of this study, no jurisdiction could demonstrate a strong and strategic coordination process between the national payments reform process, fraud prevention policy-making and the AML/CTF and sanctions policy regime.

Reflecting and expanding upon the FATF *'Partnering in the Fight Against Financial Crime'* guidelines, we recommend that countries establish a clear national economic crime data strategy that encompasses fraud, anti-money laundering and sanctions implementation considerations and actively seeks to leverage the value of central payments data. This process should involve:

- Clear objectives for tackling economic crime threats;
- A clear understanding about the data analysis and collaboration mechanisms, across public sector and private sectors, that are required to achieve the overall objectives;
- A clear understanding about the existing data-sharing opportunities and the barriers to data sharing that are relevant to those requirements;

- A commitment to support adequate legislative gateways for relevant information-sharing to address barriers and exploit opportunities;
- Ongoing coordination with payment stakeholders; and
- Constructive engagement from data protection authorities.

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

We suggest that core objectives should be to ensure that national payments rails can augment and enhance the existing national capabilities for tackling economic crime, including by:

1. Assisting regulated entities to fulfil economic crime obligations and priorities;
2. Supporting the effectiveness of third-party analytics and existing private-to-private collaboration platforms to exploit payments data; and
3. Delivering additional capabilities to national economic crime related public-private partnerships.

Leadership is essential in order to encourage payment system stakeholders to prioritise economic crime issues in the design process for national payment systems, covering:

- Fraud;
- Money laundering and terrorist financing; and
- Sanctions implementation.

Without leadership and policy coordination, there is a risk that the potential of payments infrastructure to detect economic crime will be under-explored and under-utilised. Ultimately, this will expose citizens and companies to higher levels of economic crime and reduce the national capacity to address serious and organised crime and national security priorities.

Principle 2: Legal clarity

At a basic level, countries should seek to integrate national payments infrastructure into their considerations about how to implement to best-practice guidance recommendations in the *'Partnering Against Financial Crime'* FATF report, i.e. that the public sector should:

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

For a number of use-cases described in this report, it may be possible to enable the relevant data-sharing with changes to the terms of service of the relevant payment network or other contractual arrangements, short of requiring primary legislation.

Existing legislation and public-interest provisions of data protection law may all be considered for supporting the relevant information-sharing activity. Conversely, after due consideration, new primary legislation may be deemed as essential to support and potentially oblige participation in collaborative detection frameworks through payments infrastructure. Each legal jurisdiction will need to determine the appropriate legal framework for the desired strategic results, respective to that jurisdiction.

Where an economic crime data strategy has identified the need for data-sharing requirements which are not yet clearly supported by legislation, then there should be active policy reform to ensure that legislative clarity can be achieved for the relevant data sharing.

At this stage, the constructive engagement of the data protection authority will be important to achieve the optimum balance of policy goals with regard to privacy and economic crime detection.

Principle 3: Governance and regulation

In the third principle of collaboration to tackle economic crime, policy-makers or payment system operators can consider the appropriate governance framework for enabling access to the data available at payments infrastructure.

In the case of the open API framework for accessing payments data, payments regulators or system operators may establish a governance and authorisation regime for third-parties who are accessing the data to control for relevant risks associated to:

- Data protection legal obligations;
- Cyber security protections;
- Information-security;
- Appropriate use-limitations of the data; and
- Competition law considerations.

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

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

Finally, governance frameworks will be important to ensure a right of parties adversely affected by determinations of economic crime risk to challenge the validity of those assessments. Without compromising the integrity of intelligence related to money laundering, there will need to be robust and transparent mechanisms to ensure that there is a pathway for data correction and redress should innocent parties be wrongly labelled as suspicious in a collaborative economic crime risk assessment system.[49]

Principle 4: Technology

From a technology perspective, data quality standards will be key to enable useful multi-party collaboration, including through payment rails. In jurisdictions where basic sender, beneficiary, timestamp and value information is not routinely available or reliable, there will need to be a significant policy or industry effort to raise those standards.

When adequate data standards are in place, we recommend that payment system operators and relevant authorities develop the technology framework (as well as the governance framework) for an open API structure for third parties to analyse payments data for economic crime risk. As described in this study, an open API approach can allow multiple third-parties to innovate in the use of the payments infrastructure and develop use-cases and capabilities on an agile basis, including for example across:

- Tracing and recovery of stolen funds
- Model and typology development
- Communication and investigative collaboration
- Transaction monitoring

The application of technology may also involve privacy enhancing technologies to help achieve the strategic vision, comply with relevant legislation and meet the expectations of data protection supervisors. Such technology can allow for analysis to take place without necessarily disclosing raw data that made up a collaborative computation.[50]

Principle 5: Adaptability and evolution:

As with public-private partnerships and more traditional private-to-private collaboration platforms, there will be a need to review of outputs and outcomes of the model and assess those against the strategic objectives.

The overall framework should be reviewed for effectiveness in terms of tackling economic crime, including with regard to:

- Prevention indicators for (types of) economic crime;
- The extent of tracing and investigative support to cases;
- Disruption of criminals and recovery of funds;
- Overall intelligence gains; and
- Compliance enhancements.

More broadly, as an asset for supporting a national response to economic crime threats, the performance review and accountability regime for the system should be open to public and political scrutiny.

Conclusions

Payments-level data, in isolation, will not provide an adequate framework for understanding economic crime risk.

Central payments infrastructure data will be limited to the membership of that payment system and will not be able to trace funds that flow 'off system', whether that be in cash or any number of digital wallet payments and/or virtual asset forms of payment or alternative payment rails. Payment rails will also not replace the requirement for KYC data, which is typically held by the institutions with a direct relationship with a customer or a third-party with access to that data.

The effective deployment of many economic crime typologies will require information related to a customer's behaviour and relevant identifying information derived from KYC data. Existing private-to-private collaboration platforms, such as Verafin, integrate a wide variety of types of data – covering KYC, open source, third party and other financial data – to enhance the quality of risk decisions.

However, data at the level of national payments infrastructure offers substantial advantages in terms of greater visibility of payment flows within that respective payment network compared to what a financial institution can see.

While not a 'silver bullet' for detecting economic crime, such data should be seen as offering substantial potential to augmenting and enhance the awareness of economic crime risk to private sector entities, third-party analytics providers, collaboration platforms and, potentially, also public sector stakeholders who have a responsibility to identify economic crime.

Recent innovations to unlock this data through open APIs can empower those with expertise and obligations to tackle economic crime, driving innovation and diversification in capabilities. The use-cases set out in this report are likely only a small glimpse of the opportunities that can be developed through such an approach.

Unleashing the power of payments analytics for economic crime detection promises to open a new chapter in the fight against economic crime, but it will depend on cultural and institutional willingness to bridge divides of policy making across fraud, financial crime and payments reform.

Abbreviations and Acronyms

AML/CTF (AML/CFT)	Anti-Money Laundering / Counter Terrorist Financing (Anti-Money Laundering / Combatting the Financing of Terrorism)
APIs	application programming interfaces
APP	Authorised Push Payment fraud
BCBS	The Basel Committee on Banking Supervision
BIS	The Bank for International Settlements
CDD	Customer due diligence
CPMI	Committee on Payments Market Infrastructures
EEA	European Economic Area
EFIPPP	The Europol Financial Intelligence Public Private Partnership
EPC	European Payments Council
FATF	The Financial Action Task Force
FFIS	Future of Financial Intelligence Sharing
FPAD	Fraud Pattern and Anomaly Detection
KYC	Know Your Customer (information)
NPA	UK New Payments Architecture (Pay.UK initiative)
NIBSS	Nigeria Inter-Bank Settlement System Plc
RBI	The Reserve Bank of India
RTGS	Real-time gross settlement (RTGS) payment system
RUSI	Royal United Services Institute
SCT Inst	SEPA Instant Credit Transfer
SEPA	Single Euro Payments Regulation

Endnotes

[1] Those multi-national events were:
o The 2023 Financial Action Task Force (FATF) Private Sector Consultative Forum (Vienna) 'Payments Transparency' multi-stakeholder discussion session [9 May 2023].
o 'Data Connectivity and 'Whole of System' Thinking in the UK's Architecture to Tackle Economic Crime' FFIS Roundtable (London) [2 May 2023]
o Europol Financial Intelligence Public Private Partnership (EFIPPP) Innovation Working Group (IWG) meeting focused on 'Payments analytics - Building capacity and a community of practice in Europe and beyond' (The Hague) [11 April 2023]
o 'Collaboration to Tackle Economic Crime' Nordic-Baltic Symposium (Stockholm) [3 April 2023]
o The Bank for International Settlements 'Innovation Summit' (Basel) [22 March 2023]
o 'Enhancing Fraud-Risk Alerting Through Cross-Border Payments Systems' FFIS International Practitioner Workshop (London) [15 March 2023]
o 'The Future of Private-to-Private AML Collaboration in Europe' FFIS roundtable hosted in association with Anti-Money Laundering Europe (Brussels) [28 February 2023]

[2] Financial Action Task Force (2022) *"Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing"* - https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html

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

[4] For overview information of the Europol Financial Intelligence Public Private Partnership (EFIPPP), please see https://efippp.eu/

[5] This paper uses the same definition as laid out in the "UK Economic Crime Plan 2019-2022" 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. https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version

[6] Lipis Advisors (2017) *"Fraud prevention and resolution in push payment systems, Comparative analysis"*: https://www.psr.org.uk/media/3dbln5tw/lipis-report-international-fraud-practices-msg_.pdf

[7] Financial Action Task Force (2022) *"Partnering in the Fight Against Financial Crime"* https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html

[8] See Financial Action Task Force (2022) *"Partnering in the Fight Against Financial Crime"* https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html and https://www.future-fis.com for a range of international comparative studies from 2017 on public-private and private-to-private information sharing arrangements to detect economic crime.

[9] Deloitte (2023) *"Leveraging the payments architecture in the fight against economic crime"* - Payments Architecture White Paper.

[10] The Financial Action Task Force (FATF) is the international standard setter for anti-money laundering and counter terrorist financing (AML/CFT) policy-making.

[11] Financial Action Task Force (2021) *"Opportunities and Challenges of New Technologies for AML/CFT"* - https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html

[12] Financial Action Task Force (2022) *"Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing"* https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html

[13] ibid

[14] ibid

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

[16] 2022 data from FFIS *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper (2022) - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf - supplemented by Verafin internal analysis and research submission for this study September 2023.

[17] For more details on the legal basis for private-private sharing across multiple countries, see FFIS *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper (2022) - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf

[18] See Section in this report 'The growth and limitations of current use of central payments infrastructure to detect economic crime' for more details

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

[20] Vocalink (November 2019) *"Trace and Alert Financial Crime"* Financial Crime Solutions pdf

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

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

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

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

[25] Bank for International Settlements (May 2023) *"Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders"*, p74 https://www.bis.org/publ/othp66.htm

[26] FFIS (2022) *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper, p41- https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf

[27] FFIS (2022) *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper, p44 - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf

[28] IBM, *"Payment fraud prevention at a national payment switch"* (2019) https://www.ibm.com/blog/payment-fraud-prevention-national-payment-switch/

[29] Summarised and calculated from data described in previous section.

[30] See FFIS (2022) *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper for a detailed examination of the legal basis for private-to-private information sharing for 15 different initiatives. - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf

[31] Vocalink presentation to Europol Financial Intelligence Public Private Partnership (EFIPPP) Innovation Working Group (IWG) meeting focused on *"Payments analytics - Building capacity and a community of practice in Europe and beyond"* (The Hague) [11 April 2023] with reference to Vocalink *"Trace and Alert Financial Crime"* Financial Crime Solutions pdf (November 2019)

[32] European Payments Council (EPC) (7 November 2023) *"2023 Payment Threats and Fraud Trends Report"* - https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-12/EPC181-23%20v1.0%202023%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

[33] 2022 data from FFIS *"Lessons in private-to-private financial information sharing to detect and disrupt crime"* A Survey and Policy Discussion Paper (2022) - https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-to-private_financial_information_sharing_to_detect_crime.pdf - supplemented by Verafin internal analysis and research submission for this study September 2023.

[34] Adapted from Deloitte (2023) *"Leveraging the payments architecture in the fight against economic crime"* - Payments Architecture White Paper.

[35] Pay.UK consolidated the UK's three national retail payment schemes – the Bankers Automated Clearing System (Bacs), the Faster Payment System (FPS) and the Cheque and Credit Clearing Company (now the Image Clearing System) – into a single retail interbank payment system operator.

[36] Pay.UK *"Our foundation for the future: 2021-26 Strategy"* https://newseventsinsights.wearepay.uk/media/2blffvxk/pay-uk_strategy_document.pdf

[37] Pay.UK *"Our foundation for the future: 2021-26 Strategy"* https://newseventsinsights.wearepay.uk/media/2blffvxk/pay-uk_strategy_document.pdf

[38] PYMNTS *"UK's Payment Strategy Focuses on Fraud Detection, Instant Payments"* (March, 2022) https://www.pymnts.com/news/international/2022/united-kingdom-payment-strategy-focuses-fraud-detection-instant-payments/

[39] Deloitte (2023) *"Leveraging the payments architecture in the fight against economic crime"* - Payments Architecture White Paper.

[40] CPMI (Oct 2019) *"Reducing the risk of wholesale payments fraud related to endpoint security: a toolkit"* https://www.bis.org/cpmi/publ/d188.pdf

[41] Bank for International Settlements *"Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders"* (May 2023), p11 https://www.bis.org/publ/othp66.htm

[42] Drawn from UK Payment System Regulatory commissioned international survey Lipis Advisors (2017) *"Fraud prevention and resolution in push payment systems, Comparative analysis"* and US Faster Payments Council (March 2022) *"2021 Faster Payments Fraud Survey and Report"*

[43] U.S. Federal Reserve *"FedNow Service, Fraud and instant payments: The basics"* https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html

[44] U.S. Federal Reserve *"FedNow Service, Fraud and instant payments: The basics"* https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html

[45] https://www.ebaclearing.eu/about-eba-clearing/at-a-glance/the-company/

[46] SEPA Credit Transfers and Direct Debits (STEP2) and SEPA Instant Credit Transfers (RT1) respectively

[47] https://www.ebaclearing.eu/news-and-events/media/press-releases/14-september-2023-eba-clearing-issues-specifications-and-runs-analytical-pilot-for-pan-european-fraud-pattern-and-anomaly-detection/

[48] *"Enhancing Fraud-Risk Alerting Through Cross-Border Payments Systems"* FFIS International Practitioner Workshop (London) [15 March 2023] and additional challenges expounded in Deloitte, 'Leveraging the payments architecture in the fight against economic crime' - Payments Architecture White Paper, 2023

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

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