



the payments association



# Data Sharing to prevent Economic Crime

Why you can now share data  
with confidence.

---

Supported by

**FORM3**

# Contents

- Foreword..... 3**
- Executive Summary ..... 4**
- Introduction..... 7**
- Why do we need to share data? ..... 8**
- Why is the payments industry not sharing data? ..... 8**
  - Findings from our research ..... 8
  - Data Protection and Confidentially ..... 10
- The UK’s existing regulatory framework affecting data sharing ..... 11**
- Proposed Legislation affecting data sharing in the UK ..... 13**
  - Economic Crime and Corporate Transparency Bill 2022 ..... 13
  - Data Protection and Digital Information Bill..... 14
  - Digital Identity and Attributes Trust Framework ..... 15
  - Fraud and the Justice System Report..... 16
- Data Sharing Mechanisms ..... 16**
- Examples of Data Sharing Mechanisms ..... 17**
  - Private to Public Sharing ..... 17
  - Internal Data Sharing..... 17
  - Data Sharing When Onboarding and Offboarding..... 19
  - FATF and Private-to-Private Data Sharing ..... 19
  - Broader Sharing of Fraud and Financial Intelligence..... 20
- How does the whole industry move forward on data sharing? ..... 20**
  - CIFAS and the National Fraud Database ..... 21
  - The UK and US Data Access Agreement..... 21
  - The role of the FCA ..... 22
  - The role of the Data Protection and Digital Information Bill ..... 22
  - The Rise of Smart Data ..... 23
- The Opportunities Created by Data Technology ..... 23**
  - Synthetic data ..... 23
  - Privacy Enhancing Technologies (PETs) ..... 23
  - Anglo-US Privacy Enhancing Technology (PET) prize ..... 24
- The International View ..... 24**
  - Role of the City of London ..... 24
  - Views from outside the UK ..... 26
  - Estonia ..... 26
  - The Netherlands..... 27
  - The US..... 27
  - Singapore ..... 28
- Conclusion and recommendations..... 28**
- Authors ..... 30**
- Contributors ..... 30**
- Project Financial Crime Team..... 31**
- The Payments Association ..... 32**

# Foreword

Form3 is an account-to-account payment platform that processes millions of transactions daily for clients across the UK and Europe, spanning schemes such as FPS, BACS, and SEPA. Our primary goal is to assist financial institutions in navigating the intricacies of payment processing while recognising that increased processing speed also presents challenges, such as heightened risks associated with economic crime.

When it comes to detecting, preventing and investigating economic crime there is no greater potential impact than being able to leverage the intelligence that can be gained through sharing data.

Central infrastructure and payment processing technologies like Form3 are prime locations for enabling data sharing, as data is naturally consumed in a structured manner via APIs. However, data sharing has historically been challenging to achieve due to a number of key barriers such as legislation, data inconsistency and quality, technology availability, and perceived brand risk.

This whitepaper delves into the existing barriers that prevent financial institutions from sharing data. Additionally, it examines the legislative agenda that could allow the UK to re-emerge as leaders in data innovation. We also explore the cutting-edge technologies now available to develop solutions capable of driving value from data sharing without compromising data security and compliance.

The time has finally arrived for the promise of data sharing to become a reality, with solutions providing large-scale benefits, including a major impact on the prevention of economic crime. The key to realising these benefits lies within the development of specific partnerships in the form of data sharing mechanisms. These need to be specific in terms of the problem they solve, the data required, the standards that need to be applied to that data and how the data will be handled, protected and stored using modern data privacy-enhancing technologies. The partnerships which do this most effectively will then become the most adopted which will create the largest impacts in terms of performance.

Form3 see this new data sharing ecosystem as being one of the largest innovative forces in disrupting, investigating and ultimately preventing economic crime.



**Nick Fleetwood**  
Head of Data Services

**FORM3**

# Executive Summary

## This report

Money laundering and fraud remain the biggest threats not only for consumers paying digitally, but for the growth of the payments industry and the security of the UK too. This report, produced with the support and involvement of Form3, a Benefactor of The Payments Association, examines how data is and should be shared to prevent payments-related financial crime in the UK. It reviews current and forthcoming changes to legislation, the findings of primary and secondary research by The Payments Association, and what is happening outside the UK. The report also identifies what is preventing effective data being shared to reduce economic crime. And it explores several potential ways to overcome these obstacles and effect positive change.

***“Despite legal obligations, there are not sufficient incentives to share data with other payment companies about matters such as suspicious transactions or parties to the transaction, about victims or potential victims, or about suspected or proven criminals.”***

## Findings

This report finds that criminals are getting better at defrauding consumers, avoiding detection and laundering the proceeds across both the private and public sector. In addition, it finds that the payments industry is not designed to enable or facilitate data sharing. Despite legal obligations, there are not sufficient incentives to share data with other payment companies about matters such as suspicious transactions or parties to the transaction, about victims or potential victims, or about suspected or proven criminals. As the payments industry becomes more innovative and fragmented, so identification and prevention of crime becomes harder and more expensive. Organisations outside financial services, such as telcos or retailers, are also making data sharing and crime prevention harder, and not taking responsibility for helping to solve the problem.

The report also describes how data sharing can help identify criminals and prevent crime cost-effectively, and how there is widespread industry and political support for tackling this problem by sharing data. There are several new Bills that should that make it possible for regular data sharing to become the norm. New international groups have been set up, new legislation developed, and new standards discussed recently in the UK and around the world. And a new levy on supervised firms will fund investment into a technology-based means of analysing and sharing data and reforming the UK's AML supervision regime to enable data sharing, supervise risks and enforce regulations more effectively.

## Obstacles

However, there are significant obstacles to data sharing. Legislation protecting consumers' data, privacy, confidentiality and human rights often overlap and sometimes conflict, and differ between the private and public sector. Inconsistencies between definitions and interpretation of legislation are common, and there is no accepted or adopted digital identity scheme in the UK that would make data sharing easier.

In addition, there is also no accepted, interoperable or legally compliant mechanism currently in place to enable data sharing, nor the standards and infrastructure to support it. Data in financial institutions is often inconsistent and poor quality, and regulations are complex and overlap. Fears of litigation, fines and sanctions have prevented action on this before now, as have departmental siloes in banks where fraud and crime prevention operate in different departments. And finally, the rewards for criminals are greater than the rewards for those preventing crime.

***“Now is the time to build a robust, data-driven, interoperable and centralised mechanism that enables effective data sharing through a public-private partnership.”***

## Conclusions

The report concludes that now is the time to build a robust, data-driven, interoperable and centralised mechanism that enables effective data sharing through a public-private partnership. Common standards, consistent analytical processes and a suitable and accepted liability model should be created, built and delivered by a 'scheme'. Rather than a regulator, government department or card scheme operating this scheme, it should be operated by a new institution, or one already involved with open banking, finance and data.

The report also concludes that the current Bills going through UK Parliament are welcome but not sufficient to overcome prevailing concerns about fines or penalties. Whilst the funds generated under the new levy are important, the investment of these funds must be carefully considered and monitored to ensure they result in the construction of a world class data sharing mechanism. The UK can learn from the work being carried out on standards, identity, analytical processes and a trusted liability model around the world. But to ensure that data sharing becomes a reality, strong leadership and the involvement of the public sector is now required to align attitudes across financial services, government, regulators and other sectors.

The Payments Association believes that it is time for a coordinated, whole-system response to deliver a step-change in our fight against economic crime and the criminals behind it. Such a 'whole system' response supported by strong leadership will help to remove the organisational silos preventing effective internal data sharing within and between organisations. In time, Artificial Intelligence (AI) can be deployed to reduce crime and future approaches to crime prevention should incorporate this. But now that both the legal framework and the appropriate technology exists, the UK is in a unique position to re-assume global leadership of identifying and defeating criminal activity, not just in our country but across the world.





# Introduction

The aim of this report is to examine the current arrangements for data sharing to prevent financial crime in the UK. This is achieved, firstly, by highlighting the changes that are likely to be introduced following the passing into law of the relevant provisions of the 'Economic Crime and Corporate Transparency Bill' and the 'Data Protection and Digital Information Bill', which should pave the way for better data sharing for the payments and wider financial services industry.

*"Economic crime is, in short, the crime of our times, and is increasingly being recognised as a threat to the UK's national security."*

Beyond this, the report examines some initiatives from around the world that are encouraging better data sharing, and which provide valuable lessons for the UK. The research within this report, and its recommendations for key industry stakeholders, are driven by the findings from an in-depth qualitative survey issued to members of The Payments Association, and a series of qualitative interviews with specifically chosen public and private stakeholders including Cardiff University, The Dark Money Files, Featurespace, Lancaster University, NatWest, Pay.UK, RUSI, Revolut, Salv, Sidley Austin, Stephenson Harwood LLP and Tide.

**Global estimates suggest \$2 trillion is laundered annually and fraud is now at epidemic levels.** Illicit finance has become one of the world's most prevalent businesses. As Helena Wood and Karen Baxter, authors of RUSI's report '**Towards a New Model for Economic Crime Policing**' explain, "economic crime is, in short, the crime of our times, and is increasingly being recognised as a threat to the UK's national security."

Also, whilst fraud has been addressed by both public and private platforms for decades, as more consumers take a 'digital-first' approach to their daily lives, this digitisation has also disproportionately provided attractive opportunities for criminals to exploit. The House of Commons Committee report, '**Fraud and the Justice System**' states: "Fraud has become the most commonly experienced crime in England and Wales, now accounting for more than 40% of all recorded crime. This has been facilitated by increases in cyber-crime, with the Office for National Statistics (ONS) estimating that approximately 53% of all fraud is now online-enabled."

A clear way to address this epidemic of economic crime is through better data sharing across Financial Institutions (FIs) and with, and within, the public sector. Yet, the sheer volume and complexity of laws and legislation – both primary and secondary – constrains the ability of AML-regulated entities in the financial sector from sharing information and, therefore, reducing fraud and money laundering. It is not just the legislation which directly underpins the UK's AML/CTF regime that causes such constraints, but laws and standards covering diverse areas such as competition, data protection, digital identity, digital assets, confidentiality, smart data, encryption, open finance and more.

Most commentators agree that the very limited way the financial services industry is currently sharing information is outdated, outstripped by criminals and must be vastly improved if we want to stop this rising tide of economic crime. A robust and data-driven (preferably global) solution, which addresses the issue of both fraud and money laundering, is seen as critical.

However, it is not all doom and gloom, in recent months the UK government has shown the intent to create more fertile ground for data sharing to prevent economic crime. In March 2023, the 'second Economic Crime Plan' was announced, detailing plans (for 2023-2026) for the UK's strategy to tackle economic crime and also that month the Economic Crime Levy allocations were announced. The allocations are aimed at delivering benefits to the entire anti-money laundering system across both the public and private sector and will underpin the priorities set out in the public-private Economic Crime Plan which included to improved data sharing. Whether these proposals provide sufficient opportunity for cross-industry data sharing and whether they will be executed quickly enough remains to be seen.



*“Payment systems are becoming increasingly fragmented with new innovative players entering the market; this offers clear benefits to consumers but makes it even more difficult for a single institution to detect bad behaviour.”*



**Kathryn Westmore**  
Senior Research Fellow  
**RUSI**

## Why do we need to share data?

**It is widely recognised that when FIs detect suspicious activity, their understanding of that activity is limited to their perspective and may well represent only a glimpse of a wider criminal enterprise.** This constraint offers criminals the chance to use different FIs to perpetrate money laundering schemes, layering deposits of illegal funds and exploiting a lack of awareness and co-ordination between organisations and thereby to evade Anti-Money Laundering (AML) or counter-financing of terrorism (CFT) controls. Criminals will use every means possible to exploit the gaps in defences, both nationally and across borders, and to find flaws and weaknesses in both public and private systems.

For data to be truly useful, firms need to align on which use cases the data should be used to solve, how they should collaborate, use common data standards, and enable the data to be analysed using a consistent process. There must also be a clear way of dealing with the data that’s been analysed and a framework for carrying investigations forward. Customers typically have multiple accounts with different providers as well as relationships with separate divisions within the same provider. A single FI may only see as little as 15% to 25% of its own customers’ activity, which means it cannot effectively protect itself or its customers from risk of fraud, let alone help any other FIs protect themselves. There is also an obligation to identify unusual transactions and if an FI only sees a fraction of a customer’s activity, it has no baseline to judge what is “usual” activity.

There is widespread agreement that a strategy to tackle economic crime (which term in this paper includes fraud unless otherwise stated) is crucial for the UK’s economic growth and vital to its reputation as a safe place to invest and grow a business. Unfortunately, there is a lack of consensus on definitions including what activity constitutes fraud and the boundary (and overlap) between fraud and money laundering or other crimes.

However, no-one dissents from the view that the ability to share data on suspicious activity and entities is a key component for the success of this strategy. Other key pillars of AML activity include digital identity, robust company data (ideally collected using common data standards) and real-time or near real-time access to adverse information (including adverse media).

Similarly, it is universally acknowledged that collaboration between public and private sector is essential. But it is difficult to balance the need to share data appropriately for specific anti-economic crime purposes, such as identifying potential criminals, while ensuring that appropriate safeguards exist to maintain customer confidentiality and prevent abuse of the shared data by the recipients or by criminals.



*“As anyone who has completed a jigsaw will know, you need to have all the pieces in place, in order to see the picture properly. The same is true of financial crime. We need all the pieces. But, unlike a jigsaw, there are real world consequences if some of them are missing. Criminals go unpunished, people fail to be reimbursed, lives are ruined. We must complete the picture.”*



**Graham Barrow,**  
Director, **The Dark Money Files**

## Why is the payments industry not sharing data?

### Findings from our research

In February and March 2023, The Payments Association issued a survey on data sharing to its members. The survey sampled a range of FIs from scale-ups to corporates, specifically targeting individuals who work in economic crime prevention and compliance. The survey highlighted a range of barriers which FIs face when sharing data to prevent economic crime, including:

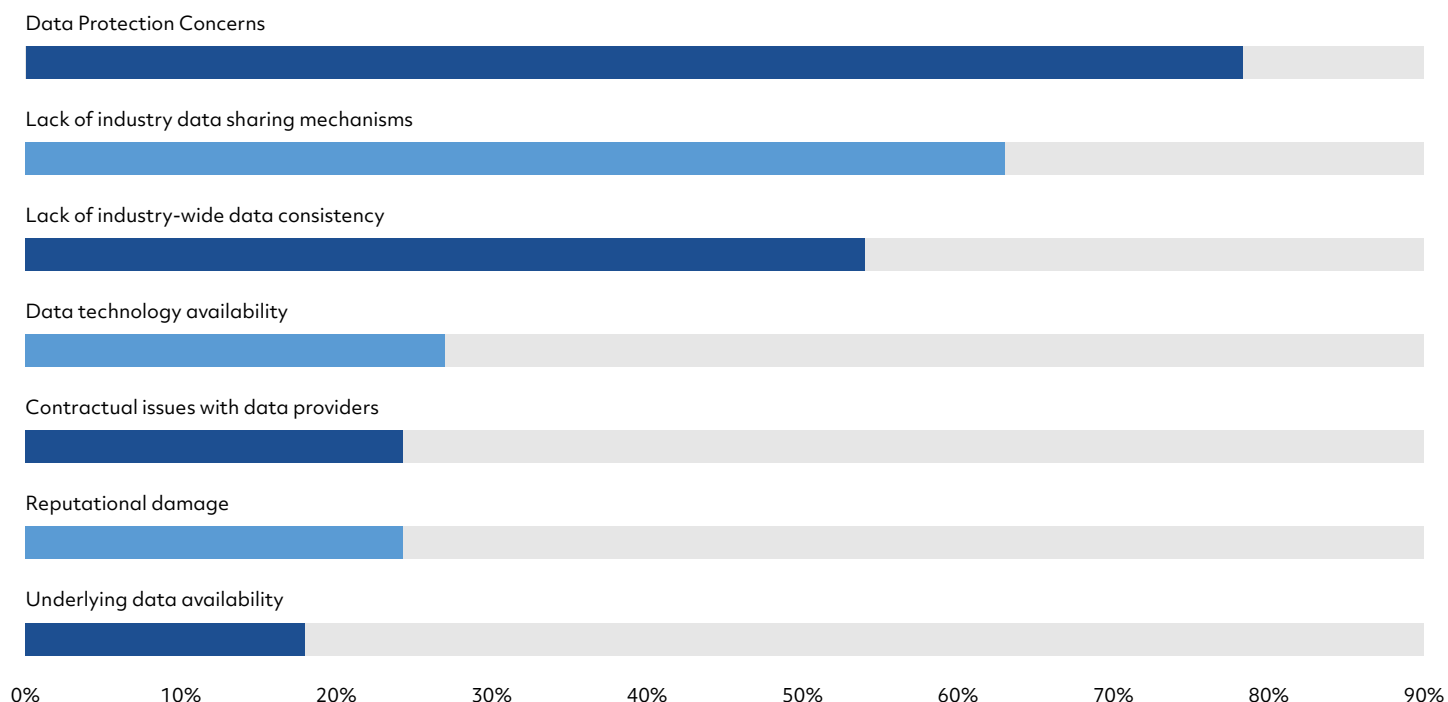
- **Balancing data privacy** and the need to share data to prevent economic crime – fear of prosecution by the ICO
- **Siloed data within firms** – this may be driven not only by technical issues but also by legislative and regulatory factors
- **Inconsistency** in the format of data
- **Inaccurate data**
- **Lack of incentives**
- **Lack of alignment** within an organisation
- **Lack of suitable infrastructure**
- **The cost** or lack of a business case for sharing



- **Economic crime** is increasingly global and cross-border
  - **Multiple data handling laws** across borders may be involved – some countries ban data sharing and punish it where it is uncovered
- **Reputational damage**
- **Brexit** was also highlighted as a barrier by some respondents. However, others suggested it now allows the UK to be more creative in the way it approaches battling financial crime

However, the seven major barriers identified by the payments industry respondents are shown in the graph below:

## In our survey



In addition to this survey, The Payments Association interviewed experts in a range of organisations, between February and March 2023, including those in tier one banks and neo-banks, technology suppliers, government departments and regulators, on data sharing and the barriers FIs face. Respondents made it clear that data sharing has to be considered in the context of the wider issues of tackling economic crime in the UK. Specifically, a lack of infrastructure was identified as a major barrier to sharing both across FIs and with, and within, the public sector.

Respondents also highlighted another major challenge for FIs as the fear of litigation from consumers (who are now much more aware of all their rights – especially privacy rights). The threat of sanctions from regulators is also holding back the legitimate sharing of data.

Even if the current proposed legislation is passed to make data sharing easier, and removes some of these fears, several problems will remain. Most FIs operate in a global market where laws on privacy and data protection differ widely. Then there are many systems involved in fighting economic crime, which are not currently interoperable. It is telling that FIs do not want to reveal which data providers they use as they are concerned that this will make them subject to greater scrutiny from the regulator. The approach of the various regulators such as the FCA and the ICO are not consistent. The interpretation of the legislation and guidance is also not consistent and often lacks clarity.

From our interviews, the larger banks consider fraud separately from other types of economic crime, i.e., the fraud department operates separately from the economic crime department. This is partly because the information they can share to prevent or identify fraud is better specified in the legislation than for economic crime in general. The burden of proof for sharing even fraud data is the same as for criminal prosecutions – it is not enough for this to be based on a suspicion or on the balance of probabilities.

The forthcoming '**Data Protection and Digital Information Bill**', which we cover later in this report, contains new types of '**Recognised Legitimate Interests**', where data controllers no longer have to conduct a 'legitimate interests' assessment, and where the benefit of the processing is assumed to be in the public interest as a matter of course. These 'Recognised Legitimate Interests' include crime "where the processing is necessary for the purposes of (a) detecting, investigating or preventing crime, or (b) apprehending or prosecuting offenders."

Given that data protection concerns are now largely addressed by this new Bill, the industry can now focus on the practical interoperability and standards, and advances in the actual technical analysis and privacy preservation of the underlying data. In this report, we explore the nature of such practical interoperability, including through models of centralised repositories, and some of the technical aspects, such as Privacy Enhancing Technologies (PETs) and Artificial Intelligence (AI). These domestic advances are seen as opening up further UK advantages on the international stage and these are already being pursued as outlined below.

And we are drawn to looking beyond our shores too, for both guidance and signs of opportunity. In January 2023, the City of London's International Regulatory Strategy Group hosted the Japanese G7 and Indian G20 presidencies to consider its priorities for 2023. Easing data flows and preventing data protectionism and localisation were identified as priorities, particularly against the backdrop of economic crime and broader sanctions busting. The move towards adoption of global standards in this regard has also been identified by many interviewees as an area where the UK could take a lead, not just through the forthcoming legislation but also due to the UK's track record in setting global security standards, such as the ISO 27000 family which is a virtual rebadging of BS 7799.

### Data Protection and Confidentiality

An important distinction between data protection and confidentiality is that data protection protects data against destruction, loss, and illegal access, whereas confidentiality allows only authorised individuals to access data. Data protection laws may help support confidentiality.

Under English law, a bank owes a duty of confidence to its customer. The contract between a bank and its customer, in the absence of agreement to the contrary, is governed by the laws of the place where the account is maintained. At the same time, this duty of confidence is matched by a duty of care under tort law, and it is this tension between the duties of confidence and care that can lie at the heart of the debate on the permitted degree of data sharing.

The recent case in the European Court of Justice (ECJ) involving **Sovim SA and the Luxembourg Business Registers** has demonstrated that a failure to properly consider data privacy has hampered European efforts to prevent financial crime. Several (formerly public) European Ultimate Beneficial Ownership (UBO) registers are now offline including those in Luxembourg, Netherlands, Germany, Austria, Ireland and Malta.

The CJEU ruling found that the EU beneficial ownership register regime, as amended by the Fifth Anti-Money Laundering Directive, was unlawful because it did not comply with the EU Charter on Fundamental Rights provisions which protect personal data and privacy. The Court held that access to beneficial ownership information went beyond what was strictly necessary to prevent or detect money laundering and terrorist financing.

Many commentators have criticised the CJEU's decision and the UK government has confirmed its intention to press ahead with the various registers of company ownership, on the basis that the UK registers adhere to the privacy requirements of the European Convention on Human Rights. In a new **policy paper** for example, the UK government has confirmed its view that the new register of overseas entities, established by the Economic Crime Transparency and Enforcement Act 2022 (and to be amended by the Economic Crime and Corporate Transparency Bill), is compliant with the privacy provisions in Article 8 of the European Convention on Human Rights, to which the UK remains a signatory.

In terms of access to personal details, safeguards built into the Bill allow individuals to ask the registrar to suppress information from the public register where, for example, that information could put them, or their household, at serious risk. Similar provisions are to be added to the UK's register of persons of significant control (PSC) and register of beneficial owners (RBO) which the government says 'will ensure that the PSC and RBO disclosure regimes do not unjustifiably establish blanket intrusions into PSCs' and RBOs' Article 8 rights.

There is yet another twist to AML developments in Europe. Until now, the European Union has laid down its AML requirements solely in the form of a Directive, leading to a minimum standard but also to different standards across the European Union. Under the new European AML regime known as AMLR, the EU plans to lay down its requirements to be fulfilled by 'obliged entities' in a directly applicable Regulation. During its latest plenary, the European Data Protection Board (EDPB) adopted a **letter** to the European Parliament, the Council and the European Commission on data sharing for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes. This letter highlights the significant risks to privacy and data protection posed by some amendments introduced by the Council, which would allow private entities, under certain conditions, to share personal data between each other for AML/CFT purposes concerning "suspicious transactions" and data collected in the course of performing customer due diligence obligations.

The EDPB expresses serious concerns about the lawfulness, necessity and proportionality of these provisions, which could result in very large-scale processing by private entities. The EDPB considers that the amendments do not adequately specify the conditions under which such processing is justified, and that they do not provide sufficient safeguards, given that such processing could have a significant impact on individuals, such as blacklisting and exclusion from financial services. The EDPB therefore recommends the co-legislators not to include these provisions in the final text of the Proposal.

## The UK's existing regulatory framework affecting data sharing

So what is the current regulatory framework for data sharing in the UK and what are the current intentions of the UK government to enable better data sharing in the public and private sectors?

In 2017 The Criminal Finances Act (CFA) introduced new sections (339ZB-339ZG) into the Proceeds of Crime Act 2002 ("POCA"), and new sections (21CA to 21CF) into the Terrorism Act 2000. These new provisions allowed banks and other businesses in the regulated sector to share information with each other on a voluntary basis in relation to a suspicion that a person is engaged in money laundering, suspicion that a person is involved in the commission of a terrorist financing offence, or in relation to the identification of terrorist property or its movement or use.

However, in the CFA 2017, as stated in RUSI's report '**Lessons in private-private financial information sharing to detect and disrupt crime**', 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 (SAR). As a result, the use of the Criminal Finances Act 2017 mechanism for private-private sharing has been "**extremely limited since its establishment.**"





It is also worth highlighting the '**Digital Economy Act**' which was designed and passed in 2017. The Act provides much of the current regulatory framework for data sharing between government agencies. Essentially, it aims to:

- Ensure clarity and consistency in how the public sector shares personal data;
- Improve public services through the better use of data; and
- Ensure data privacy.

More recently, in March 2023, the UK government published the '**second Economic Crime Plan**' covering the period 2023-2026. The plan contains the UK's strategy and commitments for tackling economic crime (including money laundering, fraud, kleptocracy and sanctions evasion). It also highlights the need for more effective collaboration, the work of existing public-private partnerships, such as the Joint Money Laundering Intelligence Taskforce, Joint Fraud Taskforce and Dedicated Card and Payment Crime Unit. Although all those interested in fighting economic crime have welcomed its publication, and the breadth of its coverage and ambition, as with the first Economic crime published in 2019, issues remain regarding resourcing and how the plan's success will be measured.

Finally, also in March 2023, as the UK government published its policy paper '**Getting ready for the Economic Levy**', which provides further clarity on 'The Economic Crime Levy (ECL)', an annual charge that applies to all organisations who are supervised under the Money Laundering Regulations (MLRs) and whose UK revenue exceeds £10.2 million per year. Amongst several allocations for this Levy, it references key investments to be made to improve data sharing over the next three years, including:

- 1 Investing over £100 million in state-of-the-art technology which will analyse and share data on threats in real time, to give law enforcement the tools it needs to stay ahead of criminals.
- 2 Investing £1.2 million for a dedicated surge team to accelerate the fundamental reform of the AML supervisory regime, leading to more effective risk-based supervision, more dissuasive enforcement, and greater sharing of high-value information and intelligence.

Admittedly, the money, collected by the FCA, will create more administration for payment firms but only for those who fall into the revenue bands below:

- Small firm (does not exceed £10.2m) -> No ECL Fee
- Medium firm (£10.2 million to £36 million) -> £10,000 ECL Fee
- Large firm (£36 million to £1 billion) -> £36,000 ECL Fee
- Very large firm – (More than £1 billion) -> £250,000 ECL Fee

We are now at a crossroads where many forces are aligning and investments being made to create the opportunity for more effective data sharing both within and across the private and public sector. There has never been more government focus on economic crime including fraud than there is today.

## Proposed Legislation affecting data sharing in the UK

### Economic Crime and Corporate Transparency Bill 2022

The Home Office's recent '**Impact Assessment on information sharing**' (January 2023), relating to the Economic Crime and Corporate Transparency Bill, explicitly recognised that businesses in the Anti-Money Laundering (AML) regulated sector (such as banks, law firms and accountants) are constrained in their ability to share information with each other and highlighted three main consequences:

- a A bank, for example, querying a particular transaction can only see its own data in relation to that transaction. It is unable to request further information from the other bank involved in the transaction to clarify relevant details. In the absence of confirmatory information, the bank may either end up under-reporting (not submitting a SAR, where the transaction is in fact suspicious) or over-reporting (submitting a SAR when in fact none was necessary).



- b** In only having access to its own data, a business is unable to spot criminal activity occurring across businesses. This is despite the fact that economic crimes such as money laundering take place across multiple bank accounts hosted by separate banks.
- c** A bank that restricts access to its products, or terminates a relationship with a customer, due to economic crime concerns, is unable to share that information with other businesses. This means that a customer whose account is terminated with a bank for economic crime reasons can easily open an account with a new provider, without the new provider being aware of the original bank's concerns. The Economic Crime and Corporate Transparency Bill 2022 contains sections on information sharing between regulated firms which are designed to encourage voluntary information sharing between firms, with the intention that this will assist in preventing or detecting economic crime, and in any subsequent investigations.

“

*“The UKs exchange of information mechanisms were largely praised by the FATF in its 2018 Mutual Evaluation Report. However, significant flaws in the exchange of information mechanisms in relation to money laundering, tax evasion, terrorism financing and fraud still exist. The recent proposed amendments are to be welcomed but data sharing must be mandatory under the Economic Crime and Corporate Transparency Bill once the data standards are set.”*



**Nicholas Ryder**

Professor in  
Financial Crime,  
School of Law and  
Politics,  
**Cardiff University**

The Bill proposes that firms in the regulated sector will be able to share customer information with other firms in the regulated sector where a firm has requested customer information and the firm with that information has taken safeguarding action in relation to that customer as a result of economic crime concerns. The proposal is that any such disclosure would not risk civil liability for a breach of customer confidentiality, provided that the disclosure of information would assist the firm receiving the information with customer due diligence/identity verification, or deciding whether to take safeguarding action. However, data protection restrictions on the information would continue to apply.

The Bill creates new provisions in the Proceeds of Crime Act 2002 (POCA) to enable sharing of information between certain businesses for the purposes of preventing, detecting and investigating economic crime.

**As currently drafted, the sharing of information under the Bill is to be entirely voluntary – there is no legal obligation to share.** Yet at the same time, the Bill introduces for the first time an offence of ‘Failure to Prevent’, and one could argue that a failure to volunteer information is tantamount to a failure of a duty of care. As the Bill continues to progress through the House of Lords, it is likely that many peers will seek to clarify the nature of these duties and the read-across to the Data Protection and Digital Information Bill (and indeed the concurrent Online Safety Bill and Financial Services and Markets Bill).

In its Impact Assessment, the government does not specify how the proposed third-party sharing platform is to operate because **“the legislation is designed to enable easier information sharing between private sector businesses, the mechanisms for which should be led by the sector itself.** The manner and form by which that information is shared may vary. It is not for the government to specify in legislation which technological solutions are most appropriate.” Whether the market is able to develop suitable third-party data sharing platforms that are fit for purpose, economically viable, interoperable and delivered in the near future is yet to be determined, and one of our industry’s most pressing challenges.

### Data Protection and Digital Information Bill

As noted previously, the results of our surveys and interviews illustrated that many respondents, who would like to be able to share data more effectively, had regulatory concerns over which data sets they were permitted to share and under what circumstances.

The publication of the **‘Data Protection and Digital Information Bill’** in March 2023, after it had been withdrawn back in October, provides the crucial legal backdrop to this report. It is worth noting that, following Machinery of government changes, the Bill now sits within the new Department of Science, Innovation and Technology, which has a greater focus on using data more effectively than might have been the case under the former Department of Digital, Culture, Media, and Sport. The delay in the resubmission of the Bill has also enabled the (formerly BEIS) Smart Data Bill team and others behind the Bill to engage more widely with industry and academic stakeholders, including through both the Authorised Push Payments Fraud TechSprint and Open Finance Policy Sprints, both hosted by FCA and PSR, and with ICO and The Payment Association’s involvement.

During the course of our research, many respondents suggested that this Bill has opened up tantalising possibilities to give Financial Services firms greater confidence in sharing data, alongside identification of the technologies necessary to handle this more effectively, as are covered under the “PET challenge” referred to later in the report.

### **All respondents welcomed the opportunity for the Bill to provide the clarity and confidence**

to enable more economic crime-related data sharing, though some respondents may wish to check the detail before welcoming ‘their obligations’ in this regard. This Bill was very timely, providing the opportunity to align Data Protection and Digital Information with the concurrent Economic Crime and Corporate Transparency Bill as well as the Financial Services and Markets Bill (covering potential abuse of crypto and digital asset classes) and the Online Safety Bill (including references to advertising of fraudulent sites). The period for consideration of the Online Safety Bill now runs until 20th July 2023.

As noted in the introduction to this report, the “catch all” in both Schedules 1 and 2 of the Data Protection Bill, relating to economic crime, are broader brush than had been expected and are reinforced by the new areas of ‘Recognised Legitimate Interests’, where controllers no longer have to conduct a ‘legitimate interests assessment’, and where the benefit of the processing is assumed to be in the public interest as a matter of course. These ‘Recognised Legitimate Interests’ will hopefully provide the industry with sufficient breadth to provide confidence, as the legislation allows for use of data under conditions citing:

---

*‘Crime 5. This condition is met where the processing is necessary for the purposes of — (a) detecting, investigating or preventing crime, or (b) apprehending or prosecuting offenders.’*

---

The current wording of the Data Protection and Digital Information (No. 2) Bill is a step in a positive direction for combatting economic crime. However, as Katie Hewson and Chloe Kite of Stephenson Harwood LLP explain, **“there will be some nervousness about data sharing that remain, pending any guidance. The draft Bill may lighten the burden by removing the need to conduct the balancing test, but data protection hurdles remain** (especially if the data sharing provisions under the Economic Crime and Corporate Transparency Bill remain voluntary)”.

Hewson and Kite go on to say that “the sharing of personal data must still be necessary for the purposes of detecting, investigating or preventing a crime – cue questions of what is necessary in this context, particularly where the inclusion of any personal data is based on a ‘suspicion’. Issues related to the sharing of criminal offence data are also likely to arise, which are unaffected by the draft Bill. It will therefore be key for FIs to think about how any ‘internal watchlists’ are compiled, as part of any data protection compliance assessment. Further, issues relating to joint controllership and the Data Sharing Code are also likely to be relevant.” Despite the positive intention of this bill there remains a need for further clarity for FIs to feel 100% confident in their ability to share data.

### **Digital Identity and Attributes Trust Framework**

The Bill also covers the practical dimensions of Digital Identity, though many organisations we spoke to noted that, without an effective liability model, a trust framework without recourse to redress could not fly commercially. Many respondents also shared their scepticism that despite a compelling case for change and industry backing, clarity and strong leadership from regulators was not assured, with references being made to the Payment Strategy Forum Financial Crime working group from 2016-19. At that time, only the ‘Guidelines for Identity Verification, Authentication and Risk Assessment’ were agreed between PSR and UK Finance, the industry body that the PSR at the time chose to lead this work for industry.

However, the Bill was seen as a welcome step in the right direction, provided that digital identification could be handled securely, in particular to allow for robust Strong Customer Authentication. Now that both parliamentary time and the underlying technology are readily available, there are fewer barriers to achieving success in 2023.

In the context of the 'Economic Crime and Corporate Transparency Bill', it was further noted that effective identification and authentication of Directors, Persons of Significant Control and Ultimate Beneficial Ownership would also need to meet such robust security standards to prevent organised crime which, as in some cases, can be merely achieved by registering illicit company formations using photo-shopped gas bills. It is also worthy of note that gas bills being used to confirm identity seemed to be a recurring theme; most supported the views of one respondent, that this 'is not exactly a hindrance to organised criminals falsifying identities for either personal or business accounts'.

Technology applications, tackling some form of economic crime through Open-Source analysis, have already sprung up and are being used to inform intelligence on both sides of the Atlantic. As our recent survey on the barriers to data sharing illustrated, few respondents believe there are technical barriers or a lack of data that could be shared. A significant barrier to data sharing is seen as a lack of industry interoperability, a function that interviewees considered should be within the central data repository. But by far the largest perceived barrier to data sharing was a fear of data protection legislation. This is a concern that one can hope has now been remedied with the imminent passing of the new Data Protection Bill.

There was a positive response to the [statement from UK Information Commissioner John Edwards](#) that the 'Data Protection and Digital Information Bill' will:

---

*"Enable organisations to grow and innovate whilst maintaining high standards of data protection rights. Data protection law needs to give people confidence to share their information to use the products and services that power our economy and society." Edwards went on to say, "we look forward to continuing to work constructively with the Government to monitor how these reforms are expressed in the Bill as it continues its journey through Parliament."*

---

### Fraud and the Justice System Report

In its response to the report on "Fraud and the Justice system", the UK government said that "sharing data is an important way to identify and disrupt fraudsters from exploiting platforms, services and people to commit their crimes". The Government is clear that this should be a priority for companies and organisations and encourages efforts in this space. The Government is taking two important steps to support information sharing to prevent economic crime.

- Firstly, GDPR establishes the prevention of fraud as a legitimate interest for sharing information. **The DCMS-led Data Protection and Digital Information Bill will make it easier for businesses to share information under GDPR** for the purposes of preventing economic crime, including fraud, by providing greater assurance around the lawful foundation a business has for sharing data.
- **Secondly, Reforms in the Economic Crime and Corporate Transparency Bill will also enable businesses, in certain situations, to share information more easily** for the purposes of preventing, investigating or detecting economic crime by disapplying civil liability for breaches of confidentiality for firms who share information to combat economic crime.

## Data Sharing Mechanisms

**The current process by which FIs share information is relatively manual and inefficient**, often relying on forms sent back and forth via email. The focus of data sharing mechanisms is also primarily focused on the investigation phase of preventing economic crime, after the crime has been committed, as opposed to focusing also on prevention.

Data Sharing mechanisms are effectively 'clubs' which FIs need to agree to join. As with any club there are certain attributes which are vital to ensure its success:

1. **The club must demonstrate clear value**, in turn motivating enough for all participants to want to join. Essentially, the product the club offers needs to be clearly defined, and the use case it solves sufficiently valuable to a cohort of participants for the club to be worth joining.
2. **The club also needs to be accessible and easy to join.** This means organisations must have shared data standards and values as well as a technology solution that does not compromise on security or performance.
3. **The value of the data sharing mechanism, the benefits of the club, will only grow as the number of participants grow with it.** This speaks to the power of the data sharing mechanism itself which manifests itself in the quality of the product that is produced.

In this way these mechanisms – or partnerships – establish themselves through effectiveness, ease of use and volume of participants.

The challenge in the early market phase of development of appropriate market mechanisms is that FIs do not necessarily know which mechanisms are going to be the most effective, so there is no consensus on value.

Later, this report explores some of the existing mechanisms which have achieved the three goals outlined above, both here in the UK and abroad.

## Examples of Data Sharing Mechanisms

### Private to Public Sharing

Suspicious Activity Reports (SARs) are the prime example of private to public sharing of data. SARs are regarded as the foundation of the UK's response to money laundering and terrorist financing. The regulated sector (e.g. banks, lawyers, accountants, estate agents) is required to submit a SAR if it knows, suspects, or has reasonable grounds for knowing or suspecting, money laundering or terrorist financing. In addition, where anyone, including those in the regulated sector, thinks they may be dealing with criminal or terrorist property and at risk of committing a money laundering or terrorist financing offence, they can submit a "request for consent". Such requests are known as a DAML (Defence Against Money Laundering) or DATF (Defence Against Terrorist Financing) SARs. In September 2022 a new power was awarded so that AML supervisors can request SARs from regulated entities.

The obligation to report discrepancies in beneficial ownership information to Companies House (a form of private to public sharing) has long been part of EU Money Laundering Directives. Essentially organisations must report inconsistencies in names, dates of birth, nationality etc., that they discover when carrying out due diligence into the beneficial owners and PSCs of customers or suppliers. From 1st April 2023, the amended Money Laundering Regulations oblige firms to report 'material' discrepancies in beneficial ownership information to Companies House at all stages of the customer lifecycle (i.e., on an ongoing basis), rather than just at onboarding.

In its report, '**Consolidated Standards on Data Sharing**', the FATF makes clear that private to public sharing is essential, citing that "sharing information concerning possible cases of abuse of the financial system with relevant authorities is one of the cornerstones of an effective AML/CFT system". The FATF's requirements on information sharing are set out in 25 of the FATF's 40 Recommendations and impact 7 immediate outcomes of the FATF Methodology for assessing effectiveness.

### Internal Data Sharing

The fragmented nature of data across multiple silos in FIs – both internally across borders and externally between providers – makes it difficult to share and interact with the data in a timely manner. Sharing across lines of business (LOBs) can be quite difficult, is seen as risky, and is avoided by many FI teams.





CONNECTION  
ANALYSIS  
DATA  
SEARCHING  
VERIFICATION  
CODING  
SENDING

20%

35%

Sept  
Nov  
Dec



In December 2022, a large **UK bank was fined by the FCA** for not sharing data internally, ironically due to fear of being fined if they had shared it. The relevant final notice revealed that teams were operating in siloes and not sharing information sufficiently. Because each team concentrated on the “fulfilment of its own function”, there was a limited understanding of how their work impacted the broader picture. Inadequate information flows between teams meant they potentially made decisions without critical information, and managers could not assess the overall position because of these information gaps. The FCA found that reports given to senior managers routinely missed vital information. For example, there was evidence that senior divisional managers were not sufficiently involved in committees where anti-money laundering risks were discussed. The case illustrates the importance of the way good management Information (MI) is linked through to information sharing on the basis that better MI leads to having better data to share.

“

*“Standardising the data that is sent between organisations (i.e. agreeing a pre-defined structure and definition) can help unlock many of the technical barriers associated with slow information exchange, allowing for quicker detection of suspicious payments.”*



**David Heron**  
Head of Standards  
Pay.UK

Article 45 of Directive (EU) 2015/849 (AMLD) requires obliged entities that are part of a group to implement group-wide policies and procedures. These group-wide anti-money laundering and countering the financing of terrorism (AML/CFT) policies and procedures, include policies and procedures for sharing information within the group for AML/CFT purposes, and are required to be implemented at the level of branches and majority-owned subsidiaries in Member States and third countries.

### Data Sharing When Onboarding and Offboarding

Data sharing when onboarding of customers takes place already, but currently it is largely at the limited level of sharing information through Credit Reference Agencies. Expansion of this into a more proactive KYC utility has been under discussion between industry and regulators for some time and formed one of the central Financial Crime recommendations of the Payments Systems Regulator’s Payment Strategy Forum back in 2017.

In regard to offboarding, the FCA’s Regulatory Sandbox explored the potential for privacy preserving sharing of information of Offboarded customers through ‘Catch the Chameleon’. This is an attempt by the participating banks to share biographic information of (rather lazy) criminals who, having had an account shut down for illicit activity, attempted to open a new account using elements of the same biographic data, such as the same email address, physical address or phone number. Given that we are all aware how simple it would be to register new companies at other addresses through abuse of Companies House onboarding, and the ease with which a new mobile phone and email address can be obtained, it is perhaps surprising that some criminals get caught out by such techniques.

Methods of blacklisting offboarded customers were frequently raised as a problem area, whilst almost all interviewees agreed that this should occur to prevent criminals simply reapplying at another institution.

### FATF and Private-to-Private Data Sharing

The FATF Standards currently require information sharing within the private sector in the context of correspondent banking, processing wire transfers, relying on third parties and implementing group-wide AML/CFT programmes.

In July 2021, the FATF published the Stocktake Report which highlighted the need for greater regulatory clarity, promotion of enabling environments, data standardisation and governance, and bias prevention in artificial intelligence for more effective AML/CTF/CPF information sharing within an appropriate DPP framework at both international and national levels. The Stocktake Report also made clear that information sharing (both private-to-private and private-to-public) is critical to fight ML/TF/PF.

In July 2022 FATF published an important report entitled **“Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing”**. This report encourages data sharing to combat economic crime and specifically recognises that “as private information sharing initiatives are piloted or progress and mature, there will be more quantitative data to assess if, when and how, this type of sharing can enhance AML/

CFT/CPF effectiveness.” The report contains a list of factors where it is potentially beneficial for private sector entities to share information for AML/CFT/CPF:

- Customer identification.
- Transaction monitoring:
- Sanctions or other screening:
- Risk understanding and management of a business relationship.
- Identification of the beneficial owner:
- Identification of typologies of crime:
- Intelligence driven inquiries

Crucially the report highlighted that data sharing can also unlock value for FIs by reducing their compliance costs.

### Broader Sharing of Fraud and Financial Intelligence

A slightly longer-term enhancement planned by firms is to increase information sharing via consortia. By the end of 2025, virtually all (99%) firms expect to be actively sharing fraud and economic crime information in this way. Greater information sharing powers and cooperation between public and private agencies would vastly improve the sector’s ability to fight economic crime. In addition, better automation, adoption of advanced analytics and AI, and a stronger relationship with supervisory bodies all promise to help transform and shape a new way of tackling economic crime.

Why does a data sharing consortia, better automation and clearer supervisory roles make so much sense?

The publication in March 2023 by Lexis Nexis Risk Solutions of a report on **‘The True Cost of Compliance’** estimated that the total economic crime compliance costs for UK financial services stood at £34.2 billion p.a. in 2023. This was a significant increase of 19% from the £28.7 billion reported almost two years earlier, and in line with the expectations of rising costs reported at the time, plus underlying cost pressures. In an interesting comparison, the report noted that this total cost is equivalent to almost three quarters of the UK’s defence budget (£45.9 billion according to government statistics) – indicating that the sector is investing a huge amount of resource to meet the UK’s economic crime compliance regulations.

Given the same report found that 22.1% of this relates to KYC/IDV checks at onboarding, that equates to over £7.5 billion per annum being spent on KYC/IDV checks that we know are largely ineffective. This is over £110 per head of the UK’s population. It appears therefore that a central repository providing more effective KYC sharing services, doing it once, but doing it properly and securely, as suggested in our surveys and research and, as explored by the Payment Strategy Forum all those years ago, could represent significant savings.

This clearly presents a case for broader sharing of economic crime intelligence. However, again, several of our interviewees flagged the lack of progress on Digital Identity as a specific barrier to effective data sharing and, following the FCA TechSprints on APP Fraud and Open Finance in recent years, it was noted that often data sharing was not even possible without appropriate consent.

### How does the industry move forward on data sharing?

Our interviews and surveys and a poll from The Payments Association’s February 2023 webinar, **‘How to combat financial crime through data sharing and collaboration,’** highlighted what industry participants thought would drive the data sharing conversation forward.

Findings from the poll and the survey produced strikingly similar results, with 79% and 81% respectively being in favour of some form of centralised repository of data for financial crime prevention, which authorised entities would be able to access and contribute to.

*“The total financial crime compliance costs for UK financial services stood at **£34.2 billion p.a.** in 2023. This was a significant increase of 19% from the **£28.7 billion** reported almost two years earlier... **this total cost is equivalent to almost three quarters of the UK’s defence budget (£45.9 billion).”***

Survey respondents were additionally asked to choose how this central repository should be formulated, whether private, public sector, or as public private partnership. Of those expressing a preference, 71% opted for a public private partnership.

Whilst there was overwhelming agreement on the basic central repository model to take forward, there was, perhaps expectedly, somewhat more of a difference of opinion on who would handle 'authorised' entities to engage with the repository and how that would be managed, what security standards would be required, and how liability would be managed across the model. Here almost everyone used the term 'scheme', and almost all respondents caveated that "scheme" should not necessarily be seen as a reference to a card scheme.

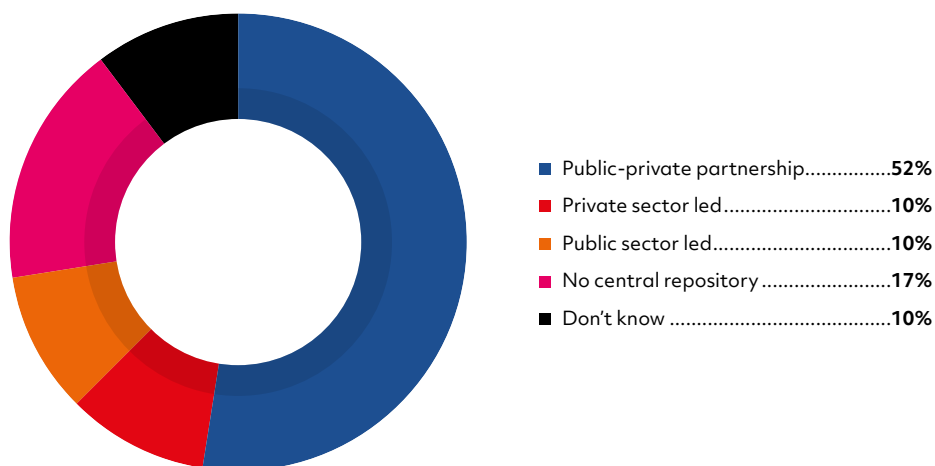
### CIFAS and the National Fraud Database

Cifas is a not-for-profit fraud prevention membership organisation. Cifas members are organisations from all sectors, sharing their data across those sectors to reduce instances of fraud and economic crime . Membership of CIFAS gives access to the National Fraud Database, a repository of fraud risk information: information can be used by CIFAS members to reduce exposure to fraud and economic crime and inform decisions according to the organisation's risk appetite.

The National Fraud Database is a reciprocal data sharing arrangement where members commit to provide data and file cases of fraud and in return receive the benefit of searching the database. Both CIFAS and its members have equal responsibility for the quality, protection and lawful use of the data submitted to and held on the National Fraud Database. Every member is responsible for the accuracy of the cases filed, and for the proportionate use of the data returned from a search.

*“A central repository providing more effective KYC sharing services, doing it once, but doing it properly and securely, as suggested in our surveys and research and, as explored by the Payment Strategy Forum all those years ago, could represent significant savings”*

### Survey - Should there be a central repository for financial crime data purposes?



### The UK and US Data Access Agreement

In October 2022 the Data Access Agreement (DAA) between the UK and US came into force. The purpose of the DAA is “to allow UK and US law enforcement to directly request data held by telecommunications providers in the other party’s jurisdiction for the exclusive purpose of preventing, detecting, investigating and prosecuting serious crimes including terrorism, child sexual abuse and exploitation”. However, the DAA has a much broader scope than just these crime types and may be used in respect of any “serious crime” which would include fraud and economic crime investigations, allowing key data to be shared much more quickly.

The types of US and UK service providers who may be ordered to provide relevant data to the authorities include a wide range of telecommunications companies, such as mobile phone companies, social media providers, cloud storage companies and messaging platforms. An Overseas Production Order (OPO) can be sought for the purpose of a serious crime investigation if there are reasonable grounds for believing the recipient has possession or control of the requested data. Failure to comply with an OPO may render the recipient in contempt of court and is likely to attract negative publicity and reputational damage.

### The role of the FCA

The FCA and PSR jointly ran an Authorised Push Payment (APP) Fraud TechSprint in September 2022. Several teams mentioned the unequal nature of the fight against APP scams – on the one hand, fraudsters who manipulate victims using sophisticated social engineering techniques and, on the other, those trying to protect customers whose messages often fall on deaf ears (not least because the fraudster knows how to combat this, for example by telling the customer to indicate that they (the fraudster) are friends or family).

### The role of the Data Protection and Digital Information Bill

In July 2022, the UK government introduced the Data Protection and Digital Information Bill detailing wide-ranging reforms to UK data protection laws, including in relation to international data transfers and legal bases for processing data. The Bill proposed amendments to various pieces of UK legislation, including the UK's incorporation of the EU's General Data Protection Regulation into domestic law (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

The Bill forms a crucial part of the UK's National Data Strategy, which aims to demonstrate post-Brexit opportunities for “unlocking the value of data” and “securing a pro-growth and trusted data regime”.

It is intended to update and simplify the UK's data protection framework to reduce burdens on organisations while maintaining high data protection standards. The governance structure and powers of the Information Commissioner's Office (the regulator) would be reformed and transferred to a new body, the Information Commission. The Bill would also:

- **Establish a framework for the provision of digital verification services** to enable digital identities to be used with the same confidence as paper documents
- **Facilitate the flow and use of personal data** for law enforcement and national security purposes

Secretary of State for Digital, Culture, Media & Sport (“DCMS”) Michelle Donelan explained: “We will be replacing GDPR with our own business and consumer-friendly British data protection system” and criticised what she considers to be the “needless regulations and business-stifling elements” of the current regime. DCMS will instead be “taking the best bits from others around the world to form a truly bespoke, British system of data protection”. As the Bill in its current form does still retain GDPR at its core, this suggests that DCMS may still intend to make significant changes to it.

The bill's impact assessment sees smart data building on the foundations of Open Banking, moving far beyond the mere extension to Open Finance. The potential inclusion of all facets of ‘Smart Data’ within the Future Entity could conceivably allow for the sharing of far more data sets, not just for the creation of a new digital economy where Fintechs become a new breed of “every-tech”, but also for the prevention of economic crime. The FCA's APP Techsprint in September 2022 assessed how sending and receiving banks could use non-financial data sets, such as social media, or telecommunications data in their risk assessment of any given transaction, helping to create a more robust payment system.

The UK will seek to incentivise investment in data sharing infrastructure, remove barriers to global data access and use, encourage data sets to be made available publicly, and boost individual control of personal data.

## The Rise of Smart Data

Smart data is digital information that is formatted so it can be acted upon at the collection point before being sent to a downstream analytics platform for further data consolidation and analytics. According to [a blog by the Centre for Data Ethics and Innovation](#), published in partnership with the UK government, Smart Data is also used to refer to the “secure sharing of customer data with authorised third-party providers (TPPs), upon the customer’s request”.

The forthcoming Data Protection and Digital Information Bill should provide the central pivot towards the adoption of a more effective economic crime data and intelligence sharing environment.

In Q4 2022 the FCA held two TechSprints, both in collaboration with the PSR and, crucially, the ICO. The first TechSprint on Authorised Push Payment Fraud looked at how industry could better protect consumers from themselves, seeking a remedy to prevent criminals using social engineering to lure consumers or businesses into actively transferring their money to accounts controlled by criminal associates. Whilst this vulnerability has long been a cause of concern, the prevalence of faster payments introduces the additional vulnerability that there is no longer a natural ‘cooling off’ period before funds are redirected elsewhere.

During the TechSprint, every team identified that the crucial factor in helping to prevent APP scams was the need for the sending or recipient bank to be able to have additional data available to ascertain whether to delay or potentially block transfers that might be higher risk. Some of these data sharing elements were purely financial – had the receiving bank seen behaviours that suggest that the account could be a mule, or, from the sending bank, was this an unusually large transfer to a new account? Many of these aspects are already in the process of being addressed through current industry initiatives, such as Confirmation of Payee (CoP), a service that checks account and reference details when a new CHAPS, Faster Payment or standing order is set up.

Other data sets that were identified as being useful included non-financial data sets, such as telco or social media data. For example, the receipt of a phone call from a new contact number immediately before a transfer might be an amber flag. A phone call from overseas, just before a transfer may be a deeper shade of amber, and a call from a known bad actor could be an obvious red flag. Yet, currently there is no incentive for other non-financial services industry sectors to share such information that most surely should fit within their own duty of care to their users.

## The Opportunities Created by Data Technology

### Synthetic data

Synthetic data generation (SDG) may be a practical privacy enhancing technology (PET) for sharing data for secondary purposes. SDG generates non-identifiable datasets that can be used and disclosed without the legislative need for additional consent given that these datasets would not be considered personal information.

### Privacy Enhancing Technologies (PETs)

In January 2022 the UN Committee of Experts on Big Data and Data Science for Official Statistics launched a pilot lab programme, to make international data sharing more secure by using PETs.

PETs have the potential to fundamentally alter the dynamics of data sharing within financial services by reducing or eliminating the privacy risks and opening the opportunities to create greater value. The World Economic Forum published a report in 2019, entitled **The Next Generation of Data Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value**, which identified five PETs that allow institutions, customers, and regulators to analyse and share insights from data without distributing the underlying data itself. These techniques are:

“

*“Preventing fraud is a priority for Revolut because we understand the damaging impact it can have on our customers’ lives. We need to see collaboration between financial institutions to make sure we’re stopping scams at their source and catching the criminals who are committing fraud. This report is a positive step towards achieving this.”*



Revolut

**Aaron Elliott-Gross,**  
Director, Group  
Head of Financial  
Crime and Fraud  
**Revolut**



**Differential privacy**, where noise is added to an analytical system so that it is impossible to reverse-engineer the individual inputs.

**Federated analysis**, where parties share the insights from their analysis without sharing the data itself.

**Homomorphic encryption**, where data is encrypted before it is shared, such that it can still be analysed but not decoded into the original information. Homomorphic encryption enables complex mathematical operations to be performed on encrypted data without compromising the encryption.

**Zero-knowledge proofs**, where users can prove their knowledge of a value without revealing the value itself.

**Secure multiparty computation**, where data analysis is spread across multiple parties such that no individual party can see the complete set of inputs.

The report states: “as these technologies mature, they will demand a re-examination of a host of mothballed data sharing projects and the exploration of previously unimaginable opportunities”.

### Anglo-US Privacy Enhancing Technology (PET) prize

In September 2022, the White House Office of Science & Technology and Innovate UK launched a research challenge on designing PETs for the prevention of Economic Crime. Techniques such as homomorphic encryption were used in the early phases of this research and such techniques featured prominently in both the FCA/PSR/ICO's APP scam TechSprint and the Open Finance Policy TechSprint.

Both TechSprints stressed the crucial role that more effective data sharing has to play in tackling illicit financial (or quasi financial data) flows and identifying bad actors. Some of this research has now moved into its third phase of red teaming and stress testing the PETs designed in the earlier phases.

There seems to be a great will to share data to help fight economic crime, but it has proven difficult to determine how effective this data sharing will actually be, or how effective the various privacy-preserving technologies will be when subjected to sophisticated, AI-driven attacks. The PETs Challenge allows us to answer both questions in a transparent and unbiased way. The Challenge pits the various diverse PETs technologies against one another, first proving their worth for detecting economic crime, and then proving their robustness against sophisticated AI-capable adversaries. The answers to these questions could not be more timely. Fraudsters are tooling up with AI and the payments industry needs to do the same.

## The International View

### Role of the City of London

In January 2023, the City of London launched the International Regulatory Strategy Group (IRSG), a joint City of London Corporation and City UK co-ordination body. IRSG is exploring opportunities for Financial and Professional Services from 2023's Japanese presidency of G7 and the Indian presidency of G20. Three of the key priorities flagged were around Digital Assets, Central Bank Digital Currencies (CBDCs) and Data Flows, all set against the backdrop of economic crime and sanctions-busting. Concerns around jurisdictional data protectionism and localisation, which provide obstacles to international financial services firms sharing data even within their own organisation, are highlighted as an area to address through agreement on international data handling standards.

IRSG work on data adequacy arrangements and their role in international trade were also published in July 2022. The IRSG will have a greater focus in 2023 on economic crime, picking up the wider geopolitical priorities on sanctions-busting, including through new asset classes,

*“Concerns around jurisdictional data protectionism and localisation, which provide obstacles to international financial services firms sharing data even within their own organisation, are highlighted as an area to address.”*





and broader cyber security concerns such as those flagged by ‘the Quad’ of US, Australia, Japan, and India. Given the latter two countries chair G7 and G20 respectively and the former two form, alongside the UK, the **AUKUS** defence and security technology alliance, the City of London can take global leadership in this area as other international fora look to London for leadership in security, technology and regulation.

*“To date, more than 1,200 collaborative investigations have been undertaken via Salv’s AML bridge, with AML and fraud cases being resolved in an **average of around 15 minutes.**”*

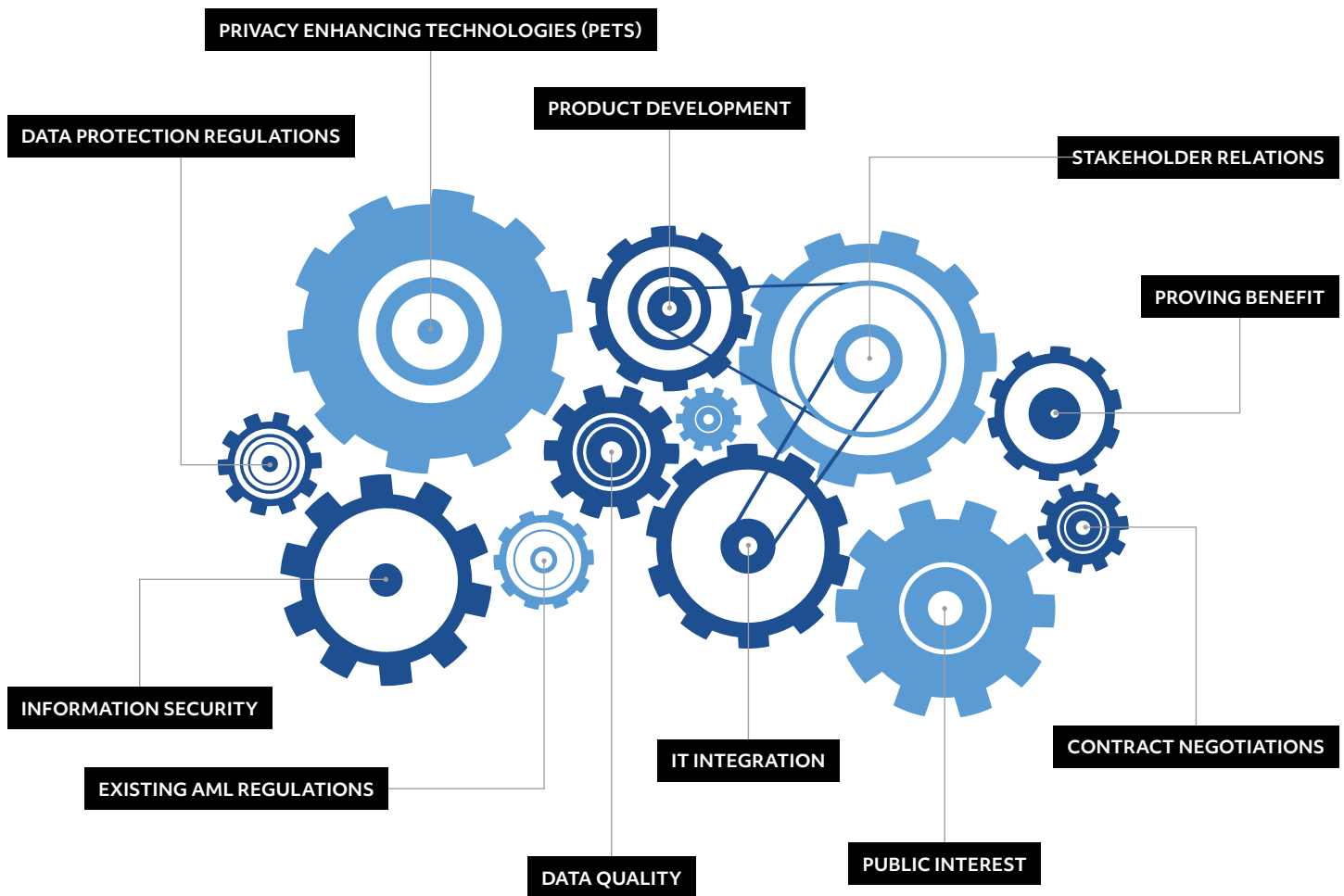
### Views from outside the UK

#### Estonia

The EU has recognised Estonia as a global leader in the digitalisation of public services, and the country continues to invest heavily in this area. Both in public and private-sector domains, workers have become familiar with carrying out all administrative tasks online which are user-centred and very accessible.

Salv, a regtech startup that uses smart technology to reduce non-compliance and economic crime founded in 2018, is headquartered in Estonia. In the image below, Salv identifies the multiple challenges which need to be addressed for organisations to fight economic crime effectively.

Salv Bridge is marketed as a secure, auditable and automatable economic crime-related information sharing platform that operates across Europe. It has been operational since July 2021 and covers both AML and fraud. It 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 exchanges.





Interestingly, Salv Bridge has been adopted by the vast majority (99%) of the Estonian banking community and is now live and operational in three markets – Estonia, the UK and Sweden with a fourth market set to be announced soon. The banks reported to Salv that up to €500,000 / month of customers' funds were prevented from reaching criminal controlled accounts. In all, up to €3m of customers' funds were safeguarded between July 2021 and February 2022. To date, more than 1,200 collaborative investigations have been undertaken via AML Bridge, with AML and fraud cases being resolved in an average of around 15 minutes. This is a vast improvement on the previous 24–48-hour delays often seen in the industry using other interbank messaging solutions.

**“Transactie Monitoring Nederland (TMNL)**

*is an initiative led by five Dutch banks (ABN AMRO, ING, Rabobank, Triodos Bank and the Volksbank) with an aim to deliver faster, better, more effective transaction monitoring (TM) and enhance the formal role of banks as ‘gatekeeper’ to the financial system.”*

**The Netherlands**

It is estimated that north of €16bn is laundered in the Netherlands annually, with human trafficking, narcotics trafficking and terrorist financing accounting for the majority of this national cost.

Transactie Monitoring Nederland (TMNL) is an initiative led by five Dutch banks (ABN AMRO, ING, Rabobank, Triodos Bank and the Volksbank) with an aim to deliver faster, better, more effective transaction monitoring (TM) and enhance the formal role of banks as ‘gatekeeper’ to the financial system. Together, they intend to tackle economic crime by collaboratively monitoring the banks’ payment transactions for signs that could potentially indicate money laundering and the financing of terrorism. In addition, TMNL works together with other organisations such as the Dutch Financial Intelligence Unit (FIU) and the Dutch Anti Money Laundering Centre (AMLC). This public/private collaboration enables all parties to apply greater focus in their search for suspected money-laundering and leads to better clarity on how public funds are being used effectively.

TMNL is also creating ‘smart models’ to detect potentially unusual transactions. These models are used effectively and responsibly, while aiming to exclude risks, such as discrimination, in the process. The links that these models make provide new insights into potential cases of money laundering and the financing of terrorism. The initiative now includes small multidisciplinary teams, consisting of AML experts, data scientists, data engineers, and machine learning engineers, who have been creating these models built on five key pillars: collaboration, legislation, privacy, secure data and responsibility.

**The US**

The US also offers a relatively positive outlook on data sharing; Section 314(b) of the USA PATRIOT Act (Sec 314) was drafted by Congress in 2001 to allow FIs to work with law enforcement agencies and with each other to support the common goal of deterring money laundering and terrorist financing. It provides FIs with the ability to share information with one another (under a ‘safe harbour’ that offers protections from liability) to better identify and report potential money laundering or terrorist activities. Sec 314(b) information sharing is a voluntary program, yet is resolutely encouraged by FinCEN, a bureau of the United States Department of the Treasury that collects and analyses information about financial transactions in order to combat domestic and international money laundering, terrorist financing, and other financial crimes.

On December 10, 2020, with the hope of enhancing participation and the effectiveness of the 314(b) program, FinCEN provided a welcomed clarification stating that FIs can now share information in reliance on the Section 314(b) relating to activities it suspects may involve money laundering or terrorist activity, even if the FI or association cannot identify specific proceeds of a Specified Unlawful Activity being laundered. Prior to this clarification, Section 314(b) permitted FIs to share information only in situations of suspected terrorism and money laundering.

Regarding the UK, it is also worth noting that FinCen’s 2022 Tech Sprint on intelligence sharing, which was an Anglo-US initiative, demonstrates that the US remains the most important bi-lateral partner for the UK in financial crime sharing, as well as both nation’s participation in the Five Eyes Alliance and the fact they are the two main global financial markets.



### Singapore

Singapore is demonstrating the potential to overtake the UK in terms of enabling data sharing to prevent economic crime. The Monetary Authority of Singapore (MAS) is both Singapore's central bank and integrated financial regulator. MAS works with the financial industry to develop Singapore as a dynamic international financial centre. In October 2021, MAS issued a consultation paper on the introduction of a regulatory framework and digital platform, known as COSMIC ('Collaborative Sharing of ML/TF Information & Cases') which would enable banks to share and analyse information on customers and transactions that cross material risk thresholds. The digital platform for FIs will seek to help identify and disrupt illicit networks and safeguard the financial system.

*"In fact, over 80% of members of The Payments Association cited data protection concerns as one of the key challenges preventing them from sharing data. This is why the position for FIs must be covered in both legislation and guidance."*

In March 2023, as part of its Financial Services and Markets (Amendment) Bill, the government announced its plans for a phased implementation of COSMIC over the next two years. The information-sharing framework will be jointly developed by MAS and six major commercial banks in Singapore – DBS, OCBC, UOB, SCB, Citibank, and HSBC, with the involvement of more FIs in subsequent phases. **The Minister of State, Alvin Tan**, remarked "a remaining weakness in the effective detection of illicit financial flows lies in the inability of FIs to alert each other to unusual activity in their customers' accounts. Financial criminals exploit these 'information silos'. However, he added, "this digital platform will enable FIs to conduct sharper analysis of customer behaviours and activities to detect potential illicit activities more promptly and warn each other of such activities". In contrast to the UK's approach to let the private sector create their own IT platform to share data, the public sector in Singapore is leading the way.

## Conclusion and recommendations

In light of the unprecedented and increasing levels of economic crime in the UK and recent regulatory changes, now is the time to act. The insights collected from members of The Payments Association and from our stakeholder interviews show that, despite various challenges and fears, there is a will and desire for better data sharing across the payments and financial services industry.

### The challenges of data sharing

**Thus far, FIs have lacked confidence in their ability to share data without risk of prosecution.** In fact, over 80% of members of The Payments Association cited data protection concerns as one of the key challenges preventing them from sharing data. This is why the position for FIs must be covered in both legislation and guidance. In addition, many FIs want to be able to use the latest technology and data but do not have the technical resources or are too small to make the required investment for themselves. Therefore, data providers must be included in this regulatory fold. In addition, it is essential that the government mobilises other industries to share non-financial data sets, such as telco or social media data. The way to address the future of data sharing in the fight against economic crime lies in a robust, data-driven, interoperable and centralised mechanism through a public-private partnership. Common standards, consistent analytical processes and a suitable and accepted liability model should be created, built and delivered by a 'scheme', which should be operated by a new institution, or one already involved with open banking, finance and data.

### Regulatory rescue on the horizon?

**The Data Protection and Digital Information Bill is opening up possibilities for concrete action to share data to combat financial crime.** Specifically, the Bill's new area of 'Recognised Legitimate Interests', where controllers no longer have to conduct a 'legitimate interest assessment', and where the benefit of the processing is assumed to be in public interest is a positive development. These 'Recognised Legitimate Interests' can provide the industry with sufficient confidence, as the legislation allows for use of data under conditions citing:

---

*‘Crime 5. This condition is met where the processing is necessary for the purposes of— (a) detecting, investigating or preventing crime, or (b) apprehending or prosecuting offenders.’*

---

In addition, the Economic Crime and Corporate Transparency Bill could also provide regulatory support. The Bill is expected to introduce, for the first time, an offence of ‘Failure to Prevent’, and one could argue that a failure to volunteer information is tantamount to a failure in a duty of care to prevent economic crime.

It is crucial that the industry continues to provide input and support negotiations on both Bills, which have the power to remove uncertainty and finally make data sharing across industries for the purpose of fighting economic crime a reality. The Payment Association will seek inputs from our members throughout the negotiation process in order to support the UK to reinstate its position as a global leader in effectively fighting economic crime.

### The role of the Levy in funding

**Parallel to the Bill we have the new Economic Crime Levy (ECL):** an annual charge to be levied for the 2022-2023 financial year and first collected in September 2023 from AML regulated entities whose UK revenue exceeds £10.2 million per year. This Levy is expected to raise £100m a year and the Treasury has suggested that this could help fund “new and uplifted” anti-money laundering and economic crime-tackling capabilities. The allocation of this funding must be carefully considered and monitored to ensure it gives the greatest ‘bang for HMT’s buck’. The Payment Association will monitor this development closely and keep its members abreast, ensuring that where required advocacy and opinions will be shared appropriately.

### Data sharing platforms need public sector involvement

**Policy makers are now positively encouraging the formation of an IT platform to share data, albeit only on a voluntary basis.** Such a central repository, which could significantly reduce cost for the industry, is to be created by the industry alone, but we strongly believe that public sector involvement in its creation, and the results obtained from it, are essential if it is to be the game changer it could be. In addition, sharing data via this new platform will only be fully effective if regulators and law enforcement support it and both are prepared and resourced (in terms of both skills and financially) to act on the outputs. There are lessons learned from initiatives across other countries in relation to standards, analytics and frameworks for carrying out investigations, identity and the underlying liability model. There must also be a clear way of dealing with the data that’s been analysed and a framework for carrying investigations forward.

### Time for a coordinated whole-system response

**Collaboration both between regulated entities and the public and private sector is key to progress on data sharing to prevent economic crime.** As the RUSI’s **‘Lessons in private-private financial information sharing to detect and disrupt crime’** report highlighted earlier states 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”. Delivering a step-change requires a coordinated ‘whole system’ response, strong leadership and the removal of organisational silos preventing effective internal data sharing within an organisation.

### The strive for global standards

**The UK and, in particular, the City of London are striving to establish Global Standards for data sharing.** A robust, data-driven and global solution, which addresses the issue of both fraud and money laundering is critical. Now that both the legal framework and the appropriate technology exists, the UK is in a unique position to re-assume global leadership of identifying and defeating criminal activity, not just domestically, but also globally.

## Authors



**Andrew Churchill**  
Ambassador  
The Payments Association



**Jane Jee**  
Ambassador  
The Payments Association



---

## Contributors



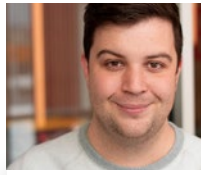
## Project Financial Crime Team



**Andrew Churchill**  
Ambassador  
The Payments  
Association



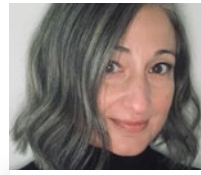
**Mitch Trehan**  
Head of UK  
Compliance &  
MLRO  
Banking Circle



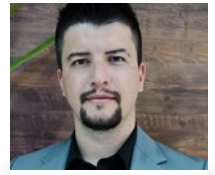
**Brendan O'Keefe**  
Enterprise sales  
Verafin



**Chryssi Chorafa**  
Founder and CEO  
StarLix



**Corinna Venturi**  
Director, Financial  
Crime  
Compliance  
Services



**Diego Harmatiuk**  
Delivery Executive  
Manager  
Qintess



**Fabien Ignaccolo**  
CEO  
Okay



**Francisco Mainez**  
Head of Financial  
Crime and  
Regulatory  
Transformation  
Lucinity



**Gregory Dellas**  
Chief Compliance  
and Innovation  
Officer  
ecommbx



**Hugo Moss**  
Business  
Development /  
International Sales  
Netcetera



**Jane Barber**  
Regulatory & Trade  
Association Lead  
NatWest



**Jane Jee**  
Ambassador  
The Payments  
Association



**John Sam-Kubam**  
SVP  
Crown Agents Bank



**Keith Stanton**  
Head of Data  
Services  
FIS



**Lucy Hawley**  
Director, Payments,  
FX and Digital,  
Global Transaction  
Banking  
Barclays



**Melanie Ockerse**  
Director Channel  
Partnerships Europe  
entersekt



**Neil Turner**  
Payments  
Compliance  
Manager  
Mastercard



**Nick Fleetwood**  
Senior Product  
Manager  
Form3



**Phil Creed**  
Director  
fscm



**Ryan Platt**  
Director of Risk and  
Compliance  
Vyne



**Sara George**  
Partner  
Sidley Austin



**Sarah Jordan**  
Director, FA -  
Forensic  
Deloitte LLP



**Serghei Minciuna**  
Director  
Salt Edge Romania



**Tim Pigott**  
Payments Industry  
Lead  
Nationwide



## About The Payments Association

The Payments Association is the largest community in payments. Founded in the UK in 2008, the association now operates communities in the UK, EU and Asia, helping almost 300 companies enhance their commercial interests, solve societal problems such as financial exclusion and evaluate new opportunities for innovation in payments.

Our purpose is to empower the most influential community in payments, where the connections, collaboration and learning shape an industry that works for all.

We operate as an independent representative for the industry and its interests, and drive collaboration within the payments sector in order to bring about meaningful change and innovation. We work closely with industry stakeholders such as the Bank of England, the FCA, HM Treasury, the Payment Systems Regulator, Pay.UK, UK Finance and Innovate Finance.

Through our comprehensive programme of activities for members and with guidance from an independent Advisory Board of

leading payments CEOs, we facilitate the connections and build the bridges that join the ecosystem together and make it stronger.

These activities include a programme of monthly digital and face-to-face events including our annual conference PAY360 and awards dinner, CEO round tables and training activities.

We run six stakeholder working Project groups: Inclusion, Regulator, Financial Crime, International Trade, Digital Currencies and Open Banking. The volunteers within these groups represent the collective view of The Payments Association members at industry-critical moments and work together to drive innovation in these areas.

We conduct exclusive industry research. This research is not legal advice. It is made available to our members through our Insights knowledge base to challenge and support their understanding of industry issues. This include monthly whitepapers, insightful interviews and tips from the industry's most successful CEOs.




the payments association

Runway East, 20 St Thomas Street, London , SE1 9RS, UK

Tel: +44 (0) 20 7378 9890

Web: [www.thepaymentsassociation.org](http://www.thepaymentsassociation.org)

Email: [info@thepaymentsassociation.org](mailto:info@thepaymentsassociation.org)

 @ThePAssoc

 [The Payments Association](#)