Royal United Services Institute
for Defence and Security Studies

Conference Report

Enabling Cross-Sector Data-Sharing to Better Prevent and Detect Scams

Kathryn Westmore, Simon Miller, Jonathan Frost and Diana Foltean

Enabling Cross-Sector Data-Sharing to Better Prevent and Detect Scams

Kathryn Westmore, Simon Miller, Jonathan Frost and Diana Foltean

RUSI Conference Report, September 2022

Royal United Services Institute
for Defence and Security Studies

191 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 191 years.

Published in 2022 by the Royal United Services Institute for Defence and Security Studies.

RUSI Conference Report, September 2022.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Introduction

FRAUD HAS BECOME a global industry. Organised large-scale volume scams, often perpetrated by international organised crime groups (OCGs), exploit the vulnerable, damage the UK's economy and undermine financial stability. The money obtained through fraud is laundered through the financial system and feeds further criminality including terrorism, human trafficking, and the trade in drugs and weapons.

The concept of data-/information sharing is cited by industry organisations, international bodies and the government as a crucial weapon in the fight against fraud. Without collaboration and data-sharing, fighting fraud has been described as 'like trying to complete a jigsaw puzzle without knowing who has the next missing piece'.[1]

Better information sharing is one of the Strategic Objectives of the UK government's current Economic Crime Plan,[2] and is likely to underpin the upcoming second iteration. While there have been a lot of welcome initiatives in the data-sharing space, particularly in relation to fraud, there remains a lack of consensus about what is meant by data-sharing, the objectives and/or incentives for the private sector to share data about frauds, and how legal and regulatory frameworks can allow for effective data-sharing, particularly between different industry sectors. There is, therefore, a clear role for industry leadership in coordinating efforts and delivering the objectives of greater and more effective data-sharing.

This Conference Report summarises the discussions at three workshops jointly facilitated by the Centre for Financial Crime and Security Studies (CFCS) at RUSI and Stop Scams UK in April and May 2022. The workshops included technical specialists from member organisations of Stop Scams UK, including banks, technology companies and telecoms providers.

The workshops were broadly focused on three themes that impact private sector entities, including Stop Scams UK members:

1. Types of scam data which can usefully be shared.
2. Barriers to sharing data effectively.
3. Practical mechanisms for sharing data.

---

1. Synectics Solutions, 'The Power of Data Sharing in Preventing Fraud', 16 January 2018, <https://www.synectics-solutions.com/our-thinking/the-power-of-data-sharing-in-preventing-fraud>, accessed 1 June 2022.
2. HM Treasury and Home Office, 'Economic Crime Plan, 2019 to 2022', 12 July 2019, <https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022>, accessed 31 May 2022.

Given the complexity of the issue of data-sharing, the aim of the workshops was to identify tangible next steps which Stop Scams UK and its members could take forward, predominantly through the establishment of bilateral and multilateral pilots between members. These should be collaborative arrangements without commercial implications. This will enable Stop Scams UK to establish a more programmatic approach to data-sharing. Throughout all discussions, participants were asked to be mindful of competition law and the need to refrain from sharing any competitively sensitive confidential information. It was also agreed by members that collaboration and data-sharing should be for the purposes of the prevention and detection of fraud and there should be no commercialisation of the shared data.

This report also makes recommendations on areas worthy of further consideration as part of the evolving debate on data-sharing, including as part of the UK government's second Economic Crime Plan, the Economic Crime Act and any changes to the UK's data privacy regime as part of the upcoming Data Reform Bill.

I. Types of Data That Can Usefully Be Shared

THE SCOPE FOR data-sharing is vast. There are 2.5 quintillion bytes of data generated a day,[3] and even if only a very small proportion of that is useful for fraud prevention and detection, it still offers enormous potential in the fight against fraud. Industry should be bold in its ambitions around the better use of this data.

The volume of data available can, however, present a challenge, particularly in identifying the data points that a particular sector or organisation can usefully share with another, especially across different sectors where there might be limited insight as to the existing data. Therefore, a better insight into the data landscape and available data points is central to understanding what data can usefully be shared, and received, across different sectors. The questions 'what data do you have?' or 'what data do you want?' do not generally yield productive discussions as it remains difficult for organisations to fully grasp the extent of their own data, let alone that of another organisation. This is particularly relevant when considering the difference between data about an actual fraud and an indicator of compromise or signal that a fraud might be about to take place.

As a result, the workshop discussions focused on working through different scam journeys, identifying at what point in the pre-payment and payment journey there were opportunities for intervention for the different Stop Scams UK members, and the specific data points that different sectors could share (or receive) to aid the prevention of the scam. This will enable the development of use cases for data-sharing focused on the outcomes of sharing in terms of the reduction in particular fraud typologies. To this end, it was important to ensure that all sectors were talking consistently about different types of scams. The different types of Authorised Push Payment (APP) scams identified as part of the Contingent Reimbursement Model (CRM) Code were viewed by participants as a good starting point (see Box 1).

A clear consensus in the discussion was that 'prevention is better than cure'. In other words, being able to stop a fraudulent payment being executed in the first place should be the primary aim of any kind of data-sharing, particularly cross-sector. Disrupting the criminal business model and reducing the return on investment of fraud in this way was seen as a desired outcome by all participants. One participant gave an example of where this type of data-sharing between sectors is proving beneficial in a collaboration between a bank and a telecoms provider to use call data to better understand what behaviour may indicate that the customer is being socially

3. Domo, 'Data Never Sleeps 5.0', <https://www.domo.com/learn/infographic/data-never-sleeps-5>, accessed 30 May 2022.

engineered to make a payment and to bypass a bank's security processes by a fraudster while on the telephone.

As noted, it was clear that stopping scams at an earlier stage requires there to be a distinction drawn between tangible intelligence about a fraud that has taken place and signals/flags that may indicate that a fraud will take place or that a particular customer is vulnerable to a fraud. There was a general view in the workshop that it would be easier to justify sharing data in the former situation but may be more difficult (although still possible) in the latter. There also may need to be a distinction drawn between data about fraud victims and data about suspected fraudsters; the legitimate use of a fraudster's personal data may be easier to justify.

Another principle established in the first workshop was the need for any new data-sharing mechanisms to use existing platforms. A number of representatives discussed their current use of MISP[4] and the National Fraud Database (NFD),[5] and expressed the view that the agreements in place that governed the use of these arrangements, including how and what information is shared and received, were a good model to use.

4. MISP Threat Sharing, <https://www.misp-project.org/>, accessed 5 July 2022.
5. CIFAS, <https://www.cifas.org.uk/fraud-prevention-community/member-benefits/data/nfd>, accessed 25 July 2022.

Box 1: Authorised Push Payment Scams

Authorised Push Payment (APP) scams occur when 'a person or business is tricked into sending money to a fraudster posing as a genuine payee'. APP scams are divided into 'malicious payee' scams and 'malicious redirection' scams.

In the former, victims are persuaded to transfer money to a payee for what they believe to be a legitimate purpose, but the fraudster absconds with the funds. Malicious payee scams include:

- Purchase fraud.
- Investment fraud.
- Advance fee fraud.
- Romance fraud.

In malicious redirection scams, the victim makes a payment to a malicious third party rather than a legitimate payee. Malicious redirection scams include:

- Invoice fraud.
- CEO fraud.
- Impersonation fraud involving bank or police staff.
- Other impersonation fraud.

Sources: Payment Systems Regulator, 'APP Scams', last updated November 2021, <https://www.psr.org.uk/our-work/app-scams/>, accessed 30 May 2022; UK Finance, '2021 Half Year Fraud Update', <https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf>, accessed 25 July 2022.

II. Barriers to Sharing Data Effectively Cross-Industry

DATA PRIVACY, AND specifically the requirements of the General Data Protection Regulation (GDPR), is often cited as a barrier to data-sharing.[6] The prospect of significant fines and potential civil liability dissuades organisations from sharing their data, especially in the absence of legal or regulatory requirements to do so.

It is clear, however, that the UK's current data protection regime allows for processing data expressly for the purposes of fraud prevention in the context of 'legitimate interests' (see Box 2). Thus, there needs to be a mindset shift from 'can I share this data?' to 'how can I share this data within the existing legal framework?'. The question of how to overcome cultural barriers to information sharing was, therefore, the focus of the second workshop, informed by examples of existing data-sharing arrangements which operate within the existing legal framework.

The need to balance concerns of data privacy with the benefits of sharing inevitably create situations which are not 'black and white'. Members acknowledged in the discussion that their organisation's willingness to share data was driven to a large extent by their risk appetite, informed by their understanding and interpretation of the relevant laws and regulations. Discussions noted that even within organisations, there is likely to be a difference in attitudes and risk appetites towards sharing between those in operational/fraud prevention roles and those in compliance/legal roles.

To support organisations, there is guidance provided by the Information Commissioner's Office (ICO) on how to carry out the necessary data protection impact assessment.[7] While the process is not overly burdensome, in the absence of any legal or regulatory incentive to share data, it is easy to understand why it is often simpler to prevent the data-sharing from happening rather than work through the mechanisms for how data can be shared, particularly when multiple institutions are involved.

---

6. For example, see the comments from some online platforms to the House of Lords Fraud Act 2006 and Digital Fraud Committee, where witnesses described how GDPR hindered data-sharing. UK Parliament, 'Fraud Act 2006 and Digital Fraud: Corrected Oral Evidence: Fraud Act 2006 and Digital Fraud', 23 May 2022, <https://committees.parliament.uk/oralevidence/10281/pdf/>, accessed 31 May 2022.
7. Information Commissioner's Office, 'Data Protection Impact Assessments', <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>, accessed 31 May 2022.

Picking up one of the themes of the first workshop, the ability to articulate the benefit of sharing a specific data point, rather than having a 'shopping list' of information that one may want to share or receive, is very powerful both in communications with the regulator and with internal stakeholders. This also demonstrates the need to start with small-scale pilot data-sharing exercises between two or three organisations which can then be expanded over time while generating a robust evidence base for the benefit of sharing the data in question. It was agreed that sharing characteristics associated with vulnerability to fraud could be very useful. However, it will, by its nature, involve sensitive information which may be more difficult to share – at least in the beginning of Stop Scams UK's data-sharing programme. This is an area where additional guidance may be helpful. The topic was explored in more detail in the third workshop.

The other area raised in discussions by members was around the level of resource required to carry out some of the data-sharing activities. Given the volume of data available, it can be a time-consuming process to assess the benefits of sharing specific data points and how to share them. Likewise, there are a number of industry initiatives, and it is not always clear where an organisation's limited resources should be best used. The evidence from smaller pilot exercises, ideally which operate alongside existing sharing mechanisms and business-as-usual activities, will undoubtedly help to demonstrate the best use of resource in this area.

Box 2: What Does 'Legitimate Interests' Mean?

Currently, Article 6(1)(f) of the GDPR provides a lawful basis for processing personal data when 'processing is necessary for the purposes of the legitimate interests', with the caveat that the processing should not override the interests and fundamental rights and freedoms of the data subject. While there is no definitive list of what constitutes a 'legitimate interest', Recital 47 states that 'processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned'.

While consideration still needs to be given to the impact of sharing personal data for the purposes of fraud, the existence of a 'legitimate interest' may make it easier to show why the sharing is necessary when balanced against any possible impact on the data subject.

Sources: Information Commissioner's Office, 'GDPR Recitals and Articles', <https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf>, accessed 10 August 2022; Information Commissioner's Office, 'What Is the "Legitimate Interests" Basis?', <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>, accessed 25 July 2022.

III. Practical Mechanisms for Sharing Data Cross-Industry

THE THIRD WORKSHOP built on the discussion in the first two and aimed to identify pilot exercises which participants could consider developing, alongside the continued sharing of insights and knowledge cross-industry to build trust between organisations.

The first area of discussion was a collaborative approach to the development of a customer propensity model, potentially via the Credit Reference Agencies (CRAs). CRAs have existing relationships with many banks, and banks are accustomed to sharing information with and using information from them. This would aim to build a broader picture of customer behaviour, reflective of the totality of a customer's financial transactions, to develop a whole-of-system model to indicate the characteristics associated with customers who are vulnerable to falling victim to fraud. This information could then be used to enable enhanced transaction monitoring of particular accounts; provide increased education to certain customers or groups of customers; and/or seek to add more friction and tailored warnings to payment journeys.

This concept prompted an interesting discussion about the value of breadth of data from multiple sources against the depth of information that a single organisation holds on an individual customer, with several participants reflecting on their own experiences with in-house models. This reflects a wider concern about the commercial incentives (or lack thereof) for data-sharing, particularly involving the mass pooling of data; if you are simply going to pay a third party to sell your data, or something less granular than your own data, back to you, what is the point? A number of participants also raised concerns about the potential impact on customers of being 'labelled' and the need for clear and open communication with customers about any such use of their data.

The second area of discussion broadly focused on the benefits of open source intelligence (OSINT) and whether all sectors could be making more and/or better use of publicly available data. An example given was the Financial Conduct Authority (FCA) Warning List,[8] which includes firms that the FCA are aware of who are operating without authorisation or carrying out fraudulent activities, including cloned firms. While this is a useful source of information, it was felt that there was more the FCA could do to improve the way in which all sectors could use the information and to allow firms to better integrate the data into their own fraud prevention and detection systems. This may include proactive notifications of when firms are added to the list, an easier way to access data points which may identify linked or related activity (such as email addresses and telephone numbers) and the proactive provision of more specific data points

8. Financial Conduct Authority, 'FCA Warning List', <https://www.fca.org.uk/scamsmart/warning-list>, accessed 31 May 2022.

to some organisations (for example, associated bank account details which may lead to the identification of more scam victims).

There were several other examples of potential data-sharing pilots which are also worthy of further consideration as part of the next phase of this work:

- Banks to explore the sharing of email addresses of known money mules to help the technology firms/social media platforms better understand mule behaviour and mule networks, and to try to identify mule herders.
- Banks to explore the sharing of voice biometric data of known fraudsters with telecoms providers to help them understand the behaviour of bad actors.
- Banks to explore the sharing of email addresses associated with business email compromise (BEC) fraud[9] with technology companies who may be able to manage accounts or even restrict access to their products and services.

9. As per the National Cyber Security Centre, BEC fraud is a type of malicious redirection fraud whereby a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information. See National Cyber Security Centre, 'Business Email Compromise: Dealing With Targeted Phishing Emails', 2020, <https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf>, accessed 31 May 2022.

IV. Next Steps

THE WORKSHOPS IDENTIFIED three recommendations for Stop Scams UK members and three recommendations for policymakers and regulators. These aim to shape the future direction of cross-industry data-sharing as well as provide policymakers with insight on how data-sharing within the private sector can be encouraged and facilitated.

Recommendations for Stop Scams UK Members

Recommendation 1: To share data effectively, organisations should be bold in their ambitions but start small. They should prioritise the small-scale exchanges of discrete data points to demonstrate the benefits of data-sharing, help overcome internal barriers and build learning. Greater coordination and leadership of the industry will be critical to helping deliver on these ambitions.

Throughout discussions, it was clear that there are still internal barriers to data-sharing within organisations which can be mitigated through exploratory bilateral discussions between firms with common goals. The workshops identified significant value in being able to demonstrate the benefits of data-sharing through small-scale exchanges of discrete data points. Not only is this more feasible from a logistical perspective but it also builds evidence for wider-scale data-sharing exercises and helps to overcome some of the reluctance to sharing. It also allows members to build a business case for data-sharing within their own organisation, including the need for additional resources where necessary.

However, it is important that organisations are ambitious in their objectives for data-sharing, and are helped in coordinating their efforts, so that momentum around projects can be built, and risk and legal advice on process shared.

Recommendation 2: To develop and prioritise a set of use cases relevant to Stop Scams UK members to help galvanise organisations and to be taken forward into pilots.

The third workshop identified a number of potential use cases/pilot exercises that could be explored and developed as part of the next stage of this work, including the development of a customer propensity model, sharing information with social media platforms to better understand mule behaviour, sharing call recordings with prior consent to better identify bad actors, and sharing email addresses associated with BEC fraud. Stop Scams UK members could potentially look to take these use cases forward alongside other priority use cases, including investment scams and crypto currency scams, in a programmatic approach to data-sharing, facilitated by Stop Scams UK.

Recommendation 3: To continually share insights and knowledge about how the threat landscape evolves and mitigations, how their industry/firm manages scams and fraud, and what data is necessary for better prevention and detection. This will be critical for building trust and confidence internally as well as in the systems and processes of other organisations.

Underpinning any future work is the need for a better understanding of the cross-sector data landscape, including an organisation's own understanding of the data points that they hold. Stop Scams UK members should take every opportunity to come together with peers and organisations in other sectors to gain a better understanding of the available data and use cases for sharing that data.

Recommendations for Policymakers and Regulators

Recommendation 4: To investigate further the cultural and behavioural barriers to data-sharing, including looking at the role that greater collaboration and leadership of the industry response to scams can play in removing these barriers. This should include looking at changes to the tone and intent of legislative and regulatory guidance to create an environment that is more permissive to responsible data-sharing, particularly of scam signal and good data.[10]

Further work is needed to understand some of the cultural barriers that are preventing organisations from sharing data. While the current legal and regulatory framework allows data-sharing for the purposes of fraud prevention, organisations and stakeholders within an organisation have very different risk appetites. There is an opportunity with future legislation and regulation to make a clearer statement of intent about the extent to which organisations should share data and to use language which creates an environment in which data-sharing is encouraged. Government should also consider the role of third-party legal advice and guidance in helping to reduce concerns around legal and regulatory jeopardy in relation to data-sharing.

Recommendation 5: To provide additional regulatory guidance to enable organisations to re-evaluate their risk appetite to the sharing of data, in particular the sharing of data that allows organisations to prevent scams by understanding individual vulnerability to scams/fraud.

The focus should be on sharing data and signals/flags which help to prevent a fraud from happening in the first place and disrupt the criminal business model. This data may either be an indication that a specific fraud is likely to take place or, at a broader level, data which allows a better understanding of a customer's vulnerability to fraud and allows organisations to put in place processes to try and prevent that individual falling victim to a scam. Additional regulatory guidance may be needed to facilitate this type of sharing given the nature of the data involved.

10. Good data is data of high quality, accurate, valid, complete and timely.

Recommendation 6: To enable greater integration between public data sources, such as the FCA Warning List, and organisations' fraud prevention and detection processes.

In general, data-sharing should not replace better use of OSINT and other available data to provide a better understanding of customers' vulnerabilities to scams, the ways in which fraud networks operate and the behaviour of bad actors. It was noted that existing sources provided by regulators, such as the FCA Warning List, could be a valuable source of information, but improvements are needed in terms of their functionality to allow organisations to better integrate it into their fraud prevention and detection processes.

About the Authors

Kathryn Westmore is a Senior Research Fellow at the Centre for Financial Crime and Security Studies (CFCS) at RUSI, where her research focuses on the UK's response to fraud, money laundering and other types of financial crime. She is a Specialist Advisor to the House of Lords Committee on the Fraud Act 2006 and Digital Fraud.

Simon Miller is the Director of Policy and Communications at Stop Scams UK. Before joining Stop Scams UK in October 2021, Simon was Head of Government Affairs at Three. Simon has also worked in senior positions across a number of government departments, including the Department for Digital, Culture, Media and Sport, the Department for Business, Energy & Industrial Strategy and also on the Leveson Inquiry into phone hacking.

Jonathan Frost is the Technical Collaborations Director at Stop Scams UK. Before joining Stop Scams UK in March 2022, Jonathan led efforts to deploy cutting-edge AI to law enforcement and public sector organisations. Jonathan has held several senior law enforcement roles that focused on countering the threat posed by economic crime. He led the delivery of the National Fraud and Cybercrime Reporting Centre, a function of the City of London Police.

Diana Foltean is the Technical Collaborations Lead at Stop Scams UK. Diana joined Stop Scams in March 2021 after working for six years in consulting at Accenture and Elixirr. As an IT Strategy consultant, she worked on digital strategy and implementation for financial services and telecommunications clients. She also led technology policy and tech for good engagements for non-profits in collaboration with the government.

191 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 191 years.

Enabling Cross-Sector Data-Sharing to Better Prevent and Detect Scams
Conference Report

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org