INNOVATE/FINANCE

A Technology Strategy to Smash Fraud

Foreword

Fraud, economic crime, and cybercrime collectively represent 50% of all crime in the UK and cause untold destruction in people's lives. Many of the points outlined in this report, if implemented, can reduce this number and prevent many of the harrowing stories affecting people and their families.

Throughout my career—whether as a regulator, practitioner, or now as a legislator, I have seen fraud from many different perspectives. At the Bank of England and the Financial Conduct Authority (FCA), I saw firsthand the scale and sophistication of financial crime, and as acting head of fraud for a FinTech, I saw just how quickly criminals' modus operandi shifts. Fraud is not a victimless crime; it devastates lives, erodes trust in our institutions, and weakens our economy. We must do whatever it takes to put an end to it.

Focusing on my role as constituency MP, my first priority is to protect people from fraudsters once and for all. I have heard heartbreaking stories from constituents—hardworking individuals who have lost their life savings, small business owners whose dreams for growth have been shattered, and families left struggling in the wake of financial deception. The pain and distress this causes are immeasurable, and it cannot continue.

Fraudsters employ increasingly sophisticated methodologies, often operating within highly structured and technologically adept organised crime networks. Effectively countering this threat requires a coordinated, cross-sector response, leveraging expertise from financial institutions, regulatory bodies, law enforcement, and policymakers alike.

This collective effort must extend from banks and businesses to policing and policy groups, from telecommunication companies to tech platforms. The Government can play a vital coordinating role in making this happen and has already made significant progress on this issue, particularly through the strong and dedicated leadership of Home Office Ministers, Dan Jarvis MP and Lord Hanson of Flint.

To effectively combat fraud at scale, I believe we should establish a national anti-fraud data centre. By uniting insights, intelligence, and expertise from across industries, this centre could serve as a formidable force against fraudsters, enabling real-time threat detection and disruption. Crucially, it could drive enhanced cross-sector data sharing, by more quickly shifting enforcement from reactive work to a strategy that is more focused on prevention, aiming to disrupt criminal operations before they even emerge.

Luke Charters MP

Labour MP for York Outer

Contents

Introduction

On behalf of FinTech firms in the UK, Innovate Finance has previously identified a critical mission in our *FinTech Plan for Government*: to make the UK the safest place in the world for digital and online transactions.[1]

A new National Fraud Strategy provides an opportunity for industry and government to take steps to make the UK the most secure place in the world for consumers and businesses to use digital finance, with a new expanded strategy to tackle the full range of threats.

This is critical to:

- **Economic growth:** The cost of payments fraud to the UK economy is at least £1.2 billion.[2] Industry data from 2023 shows that authorised push payment (APP) fraud alone accounted for 40% of all fraud losses in the UK, totalling £460 million.[3]
- **A safe and secure society:** Fraud accounts for almost two in five crimes.
- **Opportunity for all:** The impact of fraud disproportionately affects those on lower incomes[4] and 70% of victims of fraud suffer wider negative impacts including mental and physical health and debt.[5]
- **UK FinTech as a global economic champion**: High levels of fraud in the UK risks eroding consumer confidence in digital finance and is already impacting the UK's international competitiveness as a safe place to invest in FinTech and financial services.
- **Stopping wider economic crime issues:** A mechanism for data sharing and collection with clear, accountable leadership would be useful for an extended range of economic crime purposes including but not limited to money laundering and tax evasion. Fraud often funds hostile actors.
- **An opportunity to build a world beating anti-fraud technology sector:** This presents an opportunity for the UK to develop and export new anti-fraud RegTech solutions. The global fraud detection and prevention market, valued at USD 52.82 billion in 2024, is projected to reach USD 246.16 billion by 2032.[6]

In particular, there is an opening to take a new approach to data sharing, technology and technology platforms to create a technology and AI-based anti-fraud strategy which has data sharing at its core and enables the industrialisation of our fight to spot, stop and smash fraud in Britain.

This is also crucial to a number of components of UK economic goals:

- **Industrial strategy:** By building a new capability of data driven anti-fraud services.
- **Financial Services Growth and Competitiveness Strategy:** Tackling fraud has been identified by many different contributors to the HM Treasury consultation on this, and our proposals can not only strengthen the competitiveness of all financial services but will, critically, enable further innovation.[7]
- **The National Payments Vision:** The engagement panel of industry and consumer groups have universally identified tackling fraud, through data sharing and Big Tech responsibility, as a priority.
- **AI Action Plan:** UK ambitions for AI-led growth and innovation require anti-fraud protections.

The government can lead in partnership with regulators and the private sector to protect businesses and consumers when they transact online. Lessons can also be learnt from other jurisdictions, including but not limited to Singapore and Australia, in their effort to prevent and detect fraud and create a safe online environment.

We all know fraud and economic crime is a drain on the UK economy. It destroys lives, it funds hostile actors, and it is enabled on social media and telecommunications platforms. Small scale data sharing has been shown to have targeted effects. We now need to industrialise data sharing to spot and stop fraud - with enforcement agencies and tech platforms as well as financial services. To date, we have seen bilateral agreements with different parties to share data or at best law enforcement working with a small number of big banks. Data-based solutions need to be accessible and draw upon all players in the chain, including the smallest payment providers (PSPs) and the biggest tech companies.

There is clearly an assortment of diverse groups and initiatives in the fraud data sharing space which is difficult for stakeholders to keep up with. There is a vibrant cottage industry of different small initiatives, but together they do not have the critical mass or scale to crush organised fraud, let alone create a world-beating industrial sector. Not all the initiatives seem to be aware of all the other ones. We need to scale-up, connect and industrialise our approach to data sharing. There is therefore a pressing need for a National Anti Fraud Centre alongside the Economic Crime Data Strategy to bring these data sharing initiatives together and harness them in line with the government's position that *"a coordinated effort across sectors, law enforcement and government is needed"*.[8] This effort should endeavour to identify how scams can be stopped before a payment is executed, rather than simply handling post-incident issues.

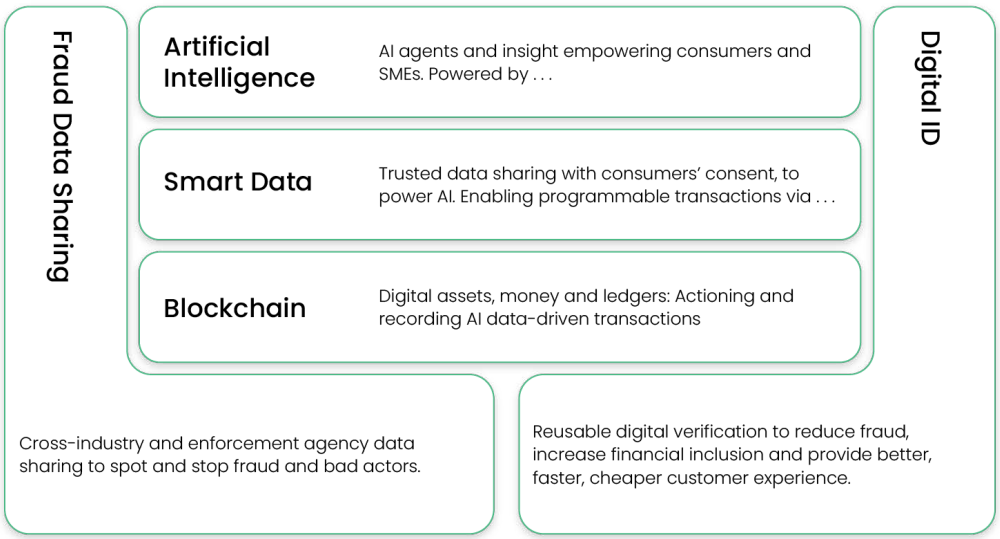
The UK also needs to end the asymmetry of data access where at present access to data to undertake fraud prevention measures is often linked to size, resources and dominance in the market. This will allow:

- Cross-industry data sharing;
- Live updates from telecommunications and tech platforms on suspected scam content and risk indicators;
- Banks and PSPs utilising data to identify, track and prevent fraudulent transactions; and
- Fraudulent transactions to be reported back to telecoms and social media platforms who can use this data to block fraudulent content.

Data sharing and data access in the financial services sector and beyond should not vary according to firms' bilateral agreements. The proposals outlined in this paper will ensure that all relevant stakeholders are involved in the process of developing a cross-industry data sharing channel. This will lay the foundation for introducing shared liability for social media and telecommunications firms in reimbursing victims of payments fraud as a means to spur action in tackling fraud at source.

Fraud data sharing should be one of five layers of a UK technology stack. Just as innovation over the last 10 years came from cloud, mobile and social technology, future growth will come from three core technologies and two enabling systems: AI, Smart Data, and Blockchain, supported by fraud data sharing and Digital ID. These five components can build a world beating UK Tech stack - a sling shot not only for financial services but also productivity and growth across the whole UK economy.

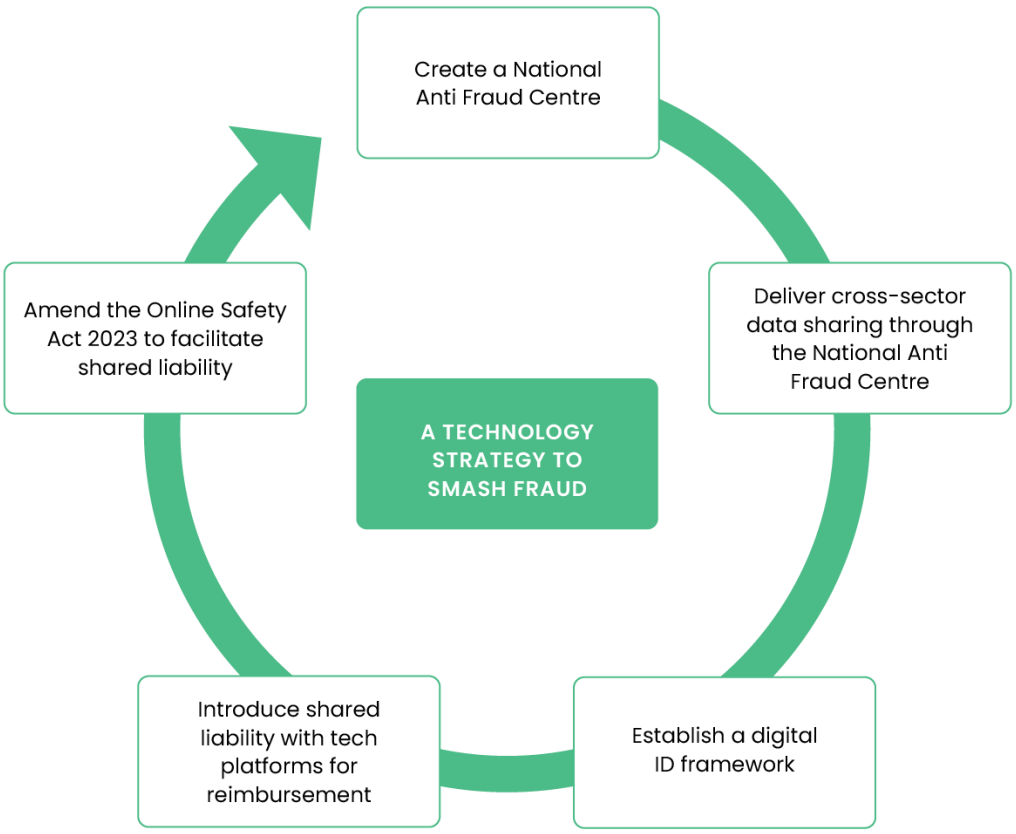
Our proposed UK Financial Tech stack:



Innovate Finance has worked with FinTech and financial services firms to develop a detailed set of proposals for a technology strategy to smash fraud. This builds on existing initiatives and what has proved to work, and looks to scale this up to an industrial level of fraud prevention, based on data sharing, joint responsibility and joined-up solutions across enforcement agencies, financial services, technology platforms and telecoms networks.

Although this paper does not cover digital ID, it is another key component of the anti-fraud strategy which we explored in our report with KPMG on *The Roadmap to Open Finance in the UK*.[9] A digital ID framework could serve as the cornerstone for secure and efficient financial transactions in an Open Data ecosystem in the UK. Reusable digital verification can enable consumers to access Smart Data and Open Finance services easily and securely, address financial inclusion and most relevant to this paper, aid in tackling fraud. Digital ID will lay the foundation for implementing advanced authentication and digital ID verification methods while ensuring compliance with the latest regulatory standards which will in turn, increase trust and confidence in digital UK financial services. A digital ID could provide a trusted mechanism that will allow mass adoption of Open Finance solutions across the ecosystem in a secure and safe manner. As the UK shifts towards this operating model, there needs to

be strong collaboration amongst market participants to promote trust and manage risk across the value chain with tackling fraud being front of mind.



Part 1: Create a National Anti Fraud Centre for cross-sector data sharing

Aims of the National Anti Fraud Centre

The aim of the National Anti Fraud Centre is to enable real-time data sharing that:

- Spots and stops fraud and related economic crime where relevant actors will be able to create better defences and more accurately block suspicious transactions;
- Works across the ecosystem to include data from tech and telecommunications platforms, payments and wider financial services firms and law enforcement;
- Is inclusive, affordable and accessible to the smallest PSPs;
- Coordinates data sharing activity and data connectivity across the ecosystem;
- Builds on what has already been done and what is in train (including but not limited to Pay.UK's Reimbursement Claims Management System (RCMS), Open Banking Limited work on transaction risk indicators, or even the UK Finance Best Practice Standards (BPS) platform and the work of organisations such as Cifas and Stop Scams UK); and
- Has resources to keep up with and stay ahead of scammers by constantly developing and updating data sharing tools.

In the rest of Part 1 below, we unpack how this can be developed and delivered in the government's forthcoming Fraud Strategy. The detail explored below serves as a 'starter-for-ten' proposal to test and prompt discussion on what is achievable.

Overview

Tackling fraud is a complex challenge that requires a large number of stakeholders across government departments, regulators, the private sector and other organisations from civil society.[10] There have been various efforts across the government and regulators to tackle fraud. For example:

- The previous government published a Fraud Strategy which sets out a plan to stop fraud at source and pursue those responsible;[11]
- The previous government also published the Economic Crime Plan 2023-2026 which included plans for an Economic Crime Data Strategy;[12]
- The soon-to-be abolished Payment Systems Regulator (PSR) introduced a mandatory reimbursement regime for APP fraud paid for by PSPs alongside other measures to combat APP fraud which includes reporting performance data;[13]
- The previous government unveiled the Online Fraud Charter which serves as a voluntary agreement between the government and the technology sector to reduce fraud on their platforms and services;[14]
- Ofcom is developing a Code of Practice to curb fraudulent advertising and working to enforce the Online Safety Act 2023 which includes provisions on fraudulent content;[15] and
- Ministers have written to tech and telecommunication sectors calling for them to go further and faster in reducing the scale of fraud taking place on their platforms and networks with an update on progress requested by March 2025 ahead of an expanded fraud strategy.[16]

Despite these measures, the sentiment felt by Innovate Finance members who span across the FinTech and financial services sector is that these efforts are siloed - with a lack of cross-cutting collaboration amongst the authorities, the private sector and other organisations from civil society. This is particularly the case when it comes to data sharing initiatives to tackle fraud at source. There are a number of initiatives being undertaken by public sector and private sector bodies to harness data sharing capabilities. However, there is no comprehensive list of data initiatives in this area which complicates the ability of stakeholders to collaborate. This demonstrates the siloed nature of how anti-fraud and data sharing

initiatives are being implemented which undermines the efficiency and success of these initiatives. It is imperative that the UK has free flow of data to assist UK law enforcement and industry to meet the challenge of combatting fraud.

Some of the initiatives currently ongoing include:

I. Action Fraud

- Action Fraud serves as the UK's national reporting centre for fraud and cybercrime.
- The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB) who are responsible for assessment of the reports and to ensure that fraud reports reach the right place.
- The police use fraud reports to build up intelligence about who is committing what fraud against whom.[17]
- The Home Office and the City of London Police are working to replace Action Fraud with a new reporting centre partly outsourced to Capita and PwC.[18] It is recognised that this seeks to increase speed, effectiveness and data quality given that *"less than 2 per cent of reports received by Action Fraud annually lead to criminal charges or prosecution"* which reflects the importance of having an effective centralised intelligence function.[19] There is no obligation for consumers or PSPs to report incidents to Action Fraud (or any other law enforcement authority) which significantly undermines the ability of law enforcement to monitor and utilise consumer data to identify trends.

II. National Crime Agency (NCA)

- The NCA works with partners from across the public, private and third sectors to pursue serious and organised fraudsters, block fraud from happening, help people avoid and recover from fraud and return funds to victims.
- It is also tasked with implementing the government's Fraud Strategy where the previous government's strategy included provisions on improving data sharing across and beyond government.[21]

- The NCA has been leading a project on data sharing with financial services - Project Fusion - but this is solely with some of the largest banks. It does not involve all banks and does not include non-bank payments providers. A far more inclusive and all-encompassing approach is needed not least as all parts of a payment chain need to be within the data sharing network.[22]

III. National Economic Crime Centre (NECC)

- Housed in the NCA, the NECC drives the UK's response to economic crime by bringing together law enforcement and justice agencies, government departments, regulatory bodies and the private sector with a shared objective of driving down serious organised economic crime.
- This includes harnessing intelligence capabilities from across the public and private sectors.[23]

IV. Public-private economic crime data strategy

- The 2023 Economic Crime Plan 2 included an action plan for developing a crime data sharing strategy.
- However, this has yet to deliver significant developments and is arguably too fragmented, is not inclusive of all industry and lacks powerful leadership and accountability that can drive delivery.[24]

V. Stop Scams UK

- Stop Scams UK is an independent industry-led collaboration funded by membership of banks, telecoms providers and tech firms who collaborate to stop scams at source.[25]
- This leads private sector collaboration between industries to enable and facilitate the development of solutions and data sharing mechanisms to combat fraud including APP scams.[26]

VI. Financial Conduct Authority (FCA) Innovation Hub

- The FCA innovation team has run a number of initiatives to stimulate data driven anti fraud solutions, including tech sprints[27], showcases [28] and providing access to a synthetic data fraud dataset[29].

VII. Cifas database

- Cifas, a not-for-profit membership association representing organisations from across the public, private and voluntary sectors, operates fraud prevention databases.
- Its National Fraud Database (NFD) is a comprehensive database of fraud risk data and intelligence in the UK, holding records of first- and third-party fraud risk including facility (account) takeover, identity fraud, false insurance claims, false applications, asset conversion and misuse of facility (which also covers causes of money muling).[30]
- Cifas members record instances of fraudulent conduct against their organisation to the relevant database, enabling other members to search against their data. When members confirm fraudulent conduct, they file their own case.[31]

VIII. Open Banking Limited transaction risk indicators

- Open Banking Limited has developed transaction risk indicators for open banking whereby secure APIs are used to enable data sharing between banks and authorised third-party providers.[32]
- This effort is aimed to reduce fraud in open banking payments and financial transactions by ensuring individuals and businesses are who they claim to be.

IX. Pay.UK Reimbursement Claims Management System (RCMS)

- In line with the role the PSR delegated to Pay.UK to oversee the mandatory reimbursement regime for APP fraud, Pay.UK has developed the RCMS.
- The RCMS is a single, whole-of-market solution designed to support PSPs with meeting their reimbursement obligations by facilitating the management of claims for PSPs by enabling sending and receiving firms to communicate with each other.[33]
- The system is also used by PSPs to meet their reporting obligations to Pay.UK who is overseeing compliance in relation to mandatory reimbursement.

While these initiatives are all positive, there is clearly an assortment of diverse groups and initiatives in the fraud data sharing space which is difficult for stakeholders to keep up with. There is a vibrant cottage industry of different small initiatives, but together they do not have the critical mass or scale to crush organised fraud, let alone create a world-beating industrial sector. Not all the initiatives seem to be aware of all the other ones. ***We need to scale-up, connect and industrialise our approach to data sharing.***

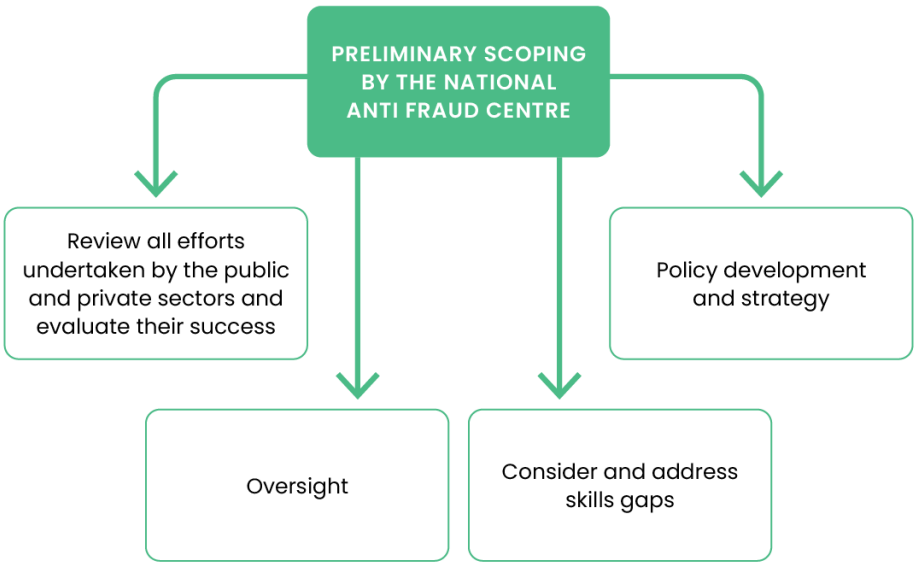
There is therefore a pressing need for a National Anti Fraud Centre alongside the Economic Crime Data Strategy to bring these data sharing initiatives together and harness them in line with the government's position that *"a coordinated effort across sectors, law enforcement and government is needed"*.[34] This effort should identify how scams can be stopped before a payment is executed, rather than simply handling post-incident issues.

Creating a National Anti Fraud Centre, loosely based on the work done in Australia, would be the appropriate vehicle to consolidate all these efforts into a single unit that will drive strategy and implementation. This will deliver:

- Central leadership across the variety of data sharing initiatives which will bring a unified and effective approach to tackling fraud at source and preventing scams from occurring;
- Development and implementation of effective data sharing and analysis between the public and private sector;
- A single consumer view of the fraud that confronted them and their vulnerability to fraud;
- A body that can undertake specific projects to address acute new types of scams;
- Coordination of effective communication with consumers on the risks of fraud and new emerging trends; and
- A unified and coordinated response from government, law enforcement and industry, as envisaged by the government.[35]

The role and responsibilities of a National Anti Fraud Centre

Preliminary scoping



In the first six months following its inception, it is suggested that the National Anti Fraud Centre should focus on the following:

I. **Review all efforts undertaken by the public and private sectors to tackle fraud and evaluate their success**

This should include efforts undertaken by financial services regulators including but not limited to the soon-to-be abolished PSR, FCA and Ofcom. It is accepted that these regulators are independent, and the purpose of the review is to identify what is being done, what is working and what could be improved. A review of the work being done by the public sector including the City of London Police as the lead force for fraud and cyber, the NCA and NECC is also necessary.

The National Anti Fraud Centre should simultaneously identify and review all efforts being undertaken by the private sector through organisations such as Stop Scams UK, other industry bodies and individual agreements between firms in relation to tackling fraud.

The goal of this review would be to outline a comprehensive list of anti-fraud and data sharing initiatives currently present, identify gaps, duplication and effectiveness in meeting their objectives, and how they can be brought together and harnessed by the National Anti Fraud Centre. There might be proven solutions such as a robust data sharing infrastructure which already exist and have been tested. The task of this review is to identify these and examine how they can be implemented on a cross-industry basis.

This is an essential first step to identifying and implementing a coordinated approach to fraud preventing fraud from occurring. It is important that this review phase moves quickly, so the National Anti Fraud Centre should set a timeframe to conclude this process and promptly begin next steps.

II. Policy development and strategy

The government has committed to publishing a new Fraud Strategy and the Economic Crime Data Strategy later in 2025. These strategies should task the National Anti Fraud Centre to develop its own strategy for coordinated central leadership focused on fraud prevention before payments are executed as well as understanding shortcomings, filling gaps (both existing and incoming) and ending duplication in data sharing initiatives by reorganising the provision of responsibilities. This must include discussions with the government on the resources needed.

The National Anti Fraud Centre should also look to develop a strategy on international coordination. This is necessary because a significant portion of fraudulent funds are sent abroad. A division that could trace fraudulent funds transferred overseas and repatriate them while bringing perpetrators to justice must be considered.

III. Oversight

The National Anti Fraud Centre should ensure that all organisations with responsibilities in the anti-fraud ecosystem are delivering on their obligations and ensure they are legally equipped to perform their tasks such as through collaboration between PSPs in data sharing before payments are executed, as well as employing tools to actively detect fraudulent payments. If there is a lack of delivery and/or legal concerns,

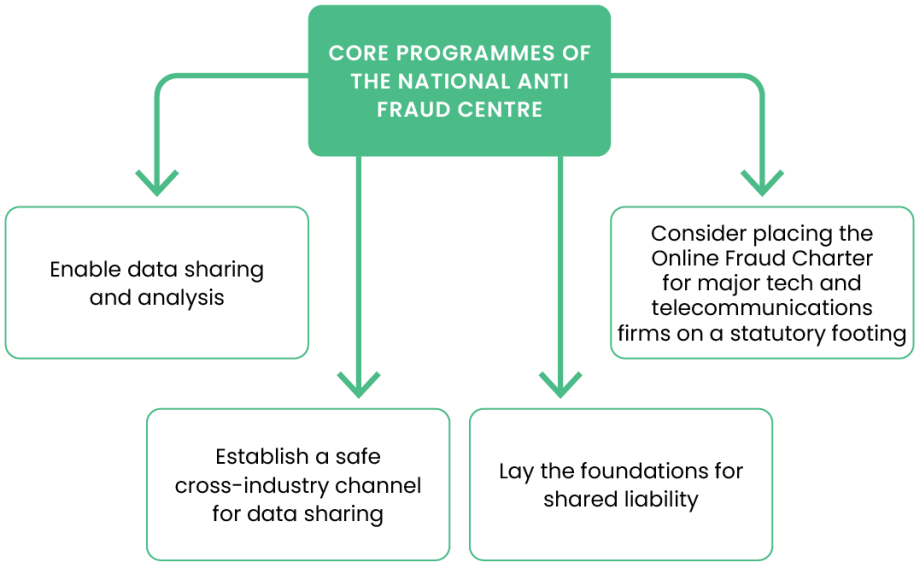
the National Anti Fraud Centre should identify the reasons behind poor delivery as well as legal issues and ambiguities that relevant authorities need to address. One area that the National Anti Fraud Centre should look into is the General Data Protection Regulation (GDPR) because it has been a source of concern for many stakeholders as an inhibitor to data sharing and analysis. Some organisations such as Cifas and regulators like the PSR have reiterated that data sharing is permissible under the GDPR to prevent fraud but given that there are stakeholders who remain concerned about its permissibility, the National Anti Fraud Centre should work with relevant authorities to clarify and explicitly permit this.

IV. Consider and address skills gaps

Fraudsters are becoming increasingly sophisticated where they also employ technology to conduct their fraudulent activities. Anti-fraud efforts, particularly data sharing to prevent scams from occurring, require individuals tasked with leading them to have the technical knowledge, skills and know-how to perform their responsibilities. This is important as technology is constantly evolving and the methods fraudsters employ to conduct their activities are constantly being updated.

Stakeholders have raised concerns that the agencies responsible to tackle fraud do not necessarily have the repertoire of skills needed to leverage technological solutions to enable and execute efficient data sharing as well as to be ahead of the technology curve in comparison to fraudsters. This is a key gap in the system that requires rectification. The National Anti Fraud Centre should therefore consider conducting a review of skills in the anti-fraud ecosystem where the existing repository of skills are considered with the aim of identifying the skills gaps that may exist, and efforts needed to fill these gaps (e.g. upskilling and recruitment) to enable effective and efficient data sharing to keep up with and stay ahead of scammers. A comparator that can be considered is cyber where there is a recognised skills and career pathway.

Core programmes



The National Anti Fraud Centre should subsequently prioritise a number of actions as suggested below:

I. Enable data sharing and analysis

Real-time data sharing, data collection and data analysis between the public and private sectors, and between PSPs and telecommunications and tech companies is pivotal to preventing fraud. This should be the raison d'être of the National Anti Fraud Centre.

It should review and propose reforms to enable data collection, data sharing and data analysis. This should include reviewing the GDPR and working with relevant authorities to deliver carve outs that will enable data sharing for the prevention of fraud and financial crime. As noted above, the GDPR has been a source of concern for many stakeholders as an inhibitor to data sharing and analysis. Some organisations such as Cifas and regulators like the PSR have reiterated that data sharing is permissible under the GDPR to prevent fraud, but given there are stakeholders who remain concerned about its permissibility, the National Anti Fraud Centre should work with relevant authorities to clarify and explicitly permit this to enable data sharing and analysis.

It should also lay out consistent principles for data sharing and ensure standards of data security and governance apply across all actors.[36] At the heart of the National Anti Fraud Centre's work on this should be to prevent scams from happening, rather than solely handling post-incident issues. This should include working with the government to stipulate the circumstances upon which data sharing between PSPs, banks and tech and telecommunications platforms is permissible (e.g. making it clear that data sharing to prevent fraud is legal and encouraged).

Fundamentally, data sharing must be reciprocal and focused on preventing fraud from occurring. This means that the aim of data sharing and analysis is not to retrospectively identify what went wrong, but rather to use real-time data to stop fraud from happening. For this to be successful, the National Anti Fraud Centre will need powers to compel all parties, including banks, PSPs, and telecommunications and tech platforms to participate in this process and do their part by providing more data in a real-time and secure manner.

II. Establish a safe cross-industry channel for data sharing

Data sharing capabilities must be built for usage by financial institutions, tech and telecommunications platforms, law enforcement and regulatory authorities.[37] There is consensus that a more coordinated and connected system or mechanism is needed given the multiplicity of data sharing initiatives present as discussed in the preceding subsections. However, there remains ongoing debate within industry on how a safe cross-industry channel for data sharing can be delivered.

On the one hand, some stakeholders believe that a single 'data lake' would not be the right response to an issue as diverse and complex as fraud notwithstanding the variety of systems being used to deliver data sharing. This is because it would be cumbersome, costly and time consuming to consolidate everything into one platform. Moreover, there is a question of strategic risk should everybody use one sole channel for data sharing in relation to all types of fraud. Increasingly, financial services and digital solutions are decentralised, enabling 'mesh' approaches and multiple real-time data sharing, drawing on ISO 20022 APIs, to build more resilient solutions that also allow for multiple service providers and faster build as opposed to monopolistic, single data warehouses.

As an option, the National Anti Fraud Centre is strongly encouraged to play a role in better connecting the series of existing and new cross-industry data sharing initiatives as a way to establish a cross-industry channel for sharing. This is sensible given the difficulties expounded on above with migrating and merging all initiatives into one system.

On the other hand, some in the payments ecosystem believe that as an option, the National Anti Fraud Centre should spearhead discussions on whether and how Pay.UK's RCMS or other equivalent systems in use for APP scams reimbursement can be utilised beyond the PSP ecosystem for real-time data sharing with fraud enablers (e.g. telecommunications and social media platforms) and law enforcement. The Centre can also review whether the categories of data inputted into these systems require review.

Nevertheless, if this is the chosen course of action, the National Anti Fraud Centre should bear in mind that the RCMS has faced significant challenges which raises some questions about whether it would be the appropriate system to take on expanded and more complex capabilities such as real-time data sharing.[38] Thus, in the event that the National Anti Fraud Centre finds the RCMS or any other equivalent system inadequate to take on expanded capabilities, it should consider the appropriate measure to establish a safe cross-industry channel for data sharing such as a new system or any other existing infrastructure that is better equipped to shoulder this capability or coordinate existing and new initiatives.

Deliberating on these options would be key to ending the asymmetry of data access where the amount of data a firm can access to undertake fraud prevention measures are encumbered by their size, resources and dominance in the market. This will allow:

- Cross-industry data sharing;
- Live updates from telecommunications platforms on suspected scam content and risk indicators;
- Banks and PSPs utilising data to identify, track and prevent fraudulent transactions; and
- Fraudulent transactions to be reported back to social media platforms who can use this data to block fraudulent content.

This will end the fragmentation in data sharing that currently exists in the financial services sector and beyond - where data sharing and data access vary according to firms' bilateral agreements and membership of various organisations. It is urged that the National Anti Fraud Centre ensures that all stakeholders are involved in the process of developing this cross-industry channel.

III. Consider placing the Online Fraud Charter for major tech and telecommunications firms on a statutory footing

The Online Fraud Charter introduced by the previous government considered data sharing by requiring signatories to work with the government, National Cyber Security Centre (NCSC), Information Commissioner's Office (ICO) and law enforcement to share information about fraud.[39]

While this Charter is welcome and a step in the right direction, its fundamental weakness is that it is voluntary and not compulsory. There appears to be no threat of penalties imposed on signatories who do not live up to the requirements of the Charter, or information on how signatories should deliver pledged actions to prevent fraud such as meeting their data sharing commitments. Moreover, some key contributors to fraud in terms of value and volume, including some of the app-based messaging services, are not signatories of the Charter.

Given the above, stakeholders in FinTech and financial services have raised two issues. Firstly, they have expressed concern about the degree to which signatories of the Charter will effectively and transparently share data and the implications of inaction on the part of non-signatories. Secondly, a FinTech firm has shared that they are still seeing the same levels of purchase scams leading to APP fraud originating from social media platforms despite the introduction of the Charter. This suggests that the set of voluntary measures for marketplaces to reduce the scale of fraud as set out in the Charter is inadequate and must be strengthened.

The National Anti Fraud Centre should therefore work with the Home Office to consider how the Charter can be strengthened and made more effective in preventing fraud. This should include updating the Charter to include obligations that improve controls on platforms such as enhancing verification requirements and requiring safe payment method access (e.g. integration with secure payment services) on online peer-to-peer

marketplaces.[40] It should also be extended to cover messaging services. The Charter should then be put on a statutory footing to compel firms to meet their obligations. Incentives such as penalties for non-compliance could also be considered.

For maximum efficiency, it can be considered whether the National Anti Fraud Centre can be made responsible for overseeing the implementation of the Charter considering the effort it will put into enhancing the Charter and how it complements its overall work in preventing fraud through data sharing. Alternatively, the National Anti Fraud Centre can work with Ofcom to evaluate how the latter can oversee the implementation of the Charter. This could entail including the Charter's provisions into the Ofcom codes of practice under the powers granted to it in the Online Safety Act 2023.

IV. Lay the foundations to introduce shared liability

With data sharing and data analysis enabled, and with the Online Fraud Charter strengthened and placed on a statutory footing, the National Anti Fraud Centre should consider how shared liability for the reimbursement of APP scam victims can be split between sending and receiving PSPs and the platform which hosted the fraud in a fair and equitable manner. This would be an additional measure that complements efforts already being undertaken and suggested in the preceding sections to prevent scams from happening before the execution of payments. It should also consider how shared liability between PSPs and tech platforms can be made practicable.

Enforcement

As the previous government acknowledged, *"fraud accounts for over 40% of crime but receives less than 1% of police resource"*.[41] Looking specifically at payments, APP fraud now accounts for 40% of all fraud losses in the UK, totalling £460 million.[42] Conversations with key stakeholders in the fight against fraud have shared anecdotally that resource or insufficient funding has been a key impediment in prioritising combatting fraud, in addition to other economic crime responsibilities.

However, shortage of resources is not the sole hindrance to enforcement. A lack of central leadership and direction could also be considered a

contributing factor. We propose that once data sharing and analysis is delivered (which includes the establishment of a cross-industry channel and shared liability), the National Anti Fraud Centre should consider bringing together law enforcement agencies, government departments, regulatory bodies and the financial services and tech sectors to deliver:

- Support for actors such as the City of London Police to target their finite resources towards areas of high harm;
- Anti-fraud policing authorities utilising data to deliver fraud prevention (i.e. data-led policing); and
- Penalties on actors who do not live up to expectations and principles set out.

These measures are necessary because law enforcement is key to delivering the objectives of the National Anti Fraud Centre.

Funding

The National Anti Fraud Centre requires a stable source of funding to be efficient. It is also recognised that funding the Centre must be done in a way that does not add pressure to public finances considering the well-documented economic headwinds the government is navigating.

Hence, it is recommended that the 'polluter pays' principle is applied whereby polluters, namely platforms and networks that have enabled fraud to thrive, should be held culpable for failing to prevent fraud. The failure of telecommunications and social media platforms to keep users safe online has necessitated a National Anti Fraud Centre. It is right that these organisations bear a share of funding the operations of the National Anti Fraud Centre.

A number of options to fund the National Anti Fraud Centre without adding pressure the public purse should be considered.

Option 1: Economic crime levy

One option is to introduce an economic crime levy across sectors including social media and telecommunications platforms to fund the operations of the National Anti Fraud Centre. This is not a novel recommendation considering there already has been an economic crime levy placed on many financial services firms since July 2023 to fund the fight against economic crime.[43] The levy proposed would make in-scope sectors contribute a portion of their revenue or profits toward fraud prevention and enforcement initiatives. In the initial years of the National Anti Fraud Centre, the scope of the levy should target all major tech and telecommunications companies with a significant user base in the UK and where high levels of fraud occur.

In December 2024, the PSR published a report on fraud origination data.[44] The data shows that nearly all fraud originates on platforms and telcos, with Meta by far the most significant one - which justifies a tech levy to incentivise firms to take action. Over time as more data emerges, it is possible that the tech levy can transition towards a risk-based model where companies in various sectors more vulnerable to fraud face higher levies.

A consultation on the size of the levy and user base of in-scope firms and sectors should be considered to determine the appropriate level of the economic crime levy set to fund the National Anti Fraud Centre.

Option 2: Enforcement receipts

Existing laws such as the Proceeds of Crime Act 2002 (POCA) enable enforcement agencies to recover the proceeds of crime and disperse those recovered funds to victims as compensation or have them reinvested to tackle economic crime more broadly. Under the Asset Recovery Incentivisation Scheme (ARIS), a proportion of confiscation order receipts are split between different departments and agencies tasked with tackling crime while remaining resources are understood to be allocated to HM Treasury as general government revenue.[45]

A mechanism could be considered for a portion of enforcement receipts to be allocated to the National Anti Fraud Centre to fund its responsibilities.

Leadership of the National Anti Fraud Centre

Option 1: Led by a senior Home Office official directly accountable to the Home Secretary

The National Anti Fraud Centre could be led by a senior official at the Home Office given that fraud falls under the department's purview. This senior official could come from the Economic Crime Directorate with a background in leading Home Office policies and initiatives on economic crime issues ranging from fraud to anti-money laundering and asset recovery which is key to understanding the issue at hand.

This official should be directly accountable to a cabinet minister, preferably the Home Secretary, given that fraud falls under the purview of the Home Office as she is responsible for leading the government's effort to create a safer country in relation to threats including fraud.

The Home Secretary should be supported by a Minister whose sole responsibility is to oversee the government's expanded Fraud Strategy (which is to be published this year), unlike the current arrangement where the Fraud Minister is responsible for several other areas including fraud.

Option 2: Led by the Fraud Minister, supported by senior Home Office officials

We recognise concerns with Option 1 whereby given the competing priorities of the Home Secretary, she might not have the bandwidth to oversee the work of the National Anti Fraud Centre that is being led by a senior Home Office official, even as tackling fraud is a key priority of senior leaders in the government.

The Fraud Minister (Minister of State at the Home Office) himself could therefore instead be tasked with leading the National Anti Fraud Centre, considering that his responsibility is tackling fraud. He will be accountable to the Home Secretary and supported by senior Home Office officials with a background in combatting economic crime.

However, stakeholders have raised concerns about the Fraud Minister's ability to currently take responsibility for leading the National Anti Fraud Centre because his responsibilities are not limited to fraud but also includes all matters relating to *"Home Office business in the Lords"* which suggests potential capacity issues.[47]

Hence, for the Fraud Minister to effectively lead this initiative on behalf of the Home Secretary, the Minister's brief might have to be streamlined where his primary focus would be tackling fraud rather than including other Home Office business.

Option 3: Led by the Anti-Fraud Champion or a new Minister

Under the previous government, there was an unpaid and voluntary role called the "Prime Minister's Anti-Fraud Champion". One of the responsibilities of the Champion was to coordinate cross-government efforts to tackle fraud and working with industry to maintain dialogue and collaboration.[48] The government could appoint an Anti-Fraud Champion to lead the National Anti Fraud Centre. The Champion could be made directly accountable to the Fraud Minister to enable parliamentary scrutiny and transparency.

The government could also consider appointing a new Minister specifically to lead the National Anti Fraud Centre. This will ensure that a government Minister can focus solely on this significant undertaking without having to streamline the existing brief of the Fraud Minister.

Measures of success

The effectiveness of the National Anti Fraud Centre in delivering its responsibilities could be judged by two metrics. This paper suggests that options to determine the measures of success can be initially based on the PSR's mandatory reimbursement regime for APP fraud. The rationale is that the data sharing focus of the National Anti Fraud Centre can directly influence fraud prevention and the financial services sector's resources while concurrently testing the merits of the strongly contested reimbursement regime.

Option 1: Halve payments fraud by 2028

The cost of payments fraud alone to the UK economy is at least £1.2 billion.[49] As noted above, industry data shows that APP fraud accounted for 40% of all fraud losses in the UK, totalling £460 million in 2023.[50] The previous government set a target of reducing overall fraud by 10% from 2019 levels in the last Parliament.[51] The UK can be more ambitious in its effort to combat fraud. The National Anti Fraud Centre should seek to halve payments fraud by 2028, or no later than 2030, as part of its responsibility to set out policy and strategy alongside enabling data sharing and analysis. 2028 is an ideal target considering that it is theoretically towards the tail end of this government's mandate. This would hence be an opportunity for the government to demonstrate its success in implementing its Fraud Strategy and creating a safer Britain that is free from threats including fraud.

The National Anti Fraud Centre should review and publish a report on its progress every 12 months. Data on its progress can be corroborated with PSR data (and subsequently FCA data following the PSR's abolition) on the volume of in-scope APP fraud reimbursement claims. The Minister responsible should notify Parliament on the findings of the review, explain shortcomings in the road to achieving the target and outline measures the Centre is taking to be on track to halve payments fraud. This level of political accountability should serve as an impetus for the Centre to focus on outcomes and drive coordinated action across government agencies, regulators and the private sector.

Option 2: Reduced industry spend on reimbursement

Regardless of whether payments fraud is set to be halved by 2028 as suggested above, the National Anti Fraud Centre will also have achieved success if data shows that the value of APP fraud reimbursement claims have reduced. A reduction in fraud levels should mean fewer APP scam reimbursement claims which should effectively mean that PSPs spend less on mandatory reimbursement (and in turn all their customers pay less for this).

This is a target that can be achieved even before shared liability with telecommunications and social media platforms is introduced. If the National Anti Fraud Centre succeeds in introducing shared liability, the

payments' industry spend on reimbursing victims on APP scams should also significantly reduce. This assumption is based on the fact that 77% of all APP fraud cases originate online according to industry data.[52]

Part 2: Introduce shared liability for social media and telecommunications firms

Overview

Social media and telecommunications are the main sources of fraud origination. Industry data shows that 77% of all APP fraud cases originate online. According to data from a FinTech firm, Meta platforms are the single largest source of fraud origination, given that fraud originating from Meta constitutes 60.5% of all reports of fraud it received, amounting to a value of 33.2% of all scams.[53] This data also shows that 61.1% of fraud cases originating from Meta platforms relate to purchase scams, while investment scams are worth 61.3% of all scams originating from Meta.[54]

Action should therefore be taken to incentivise social media and telecommunications firms to do more and tackle fraud being conducted on their platforms. PSPs are currently being held solely liable for fraud under the PSR's mandatory reimbursement regime where sending and receiving PSPs equally split the cost of reimbursing victims of fraud. Reimbursement alone does little to solve the problem of rising fraud and could encourage fraudsters to exploit the system by claiming to be victims themselves. Liability should instead be split in a fair and equitable manner between sending and receiving PSPs as set out by the soon-to-be abolished PSR, and the likes of social media and telecommunications companies.

In the rest of Part 2 below, we unpack how shared liability can be introduced and delivered. The detail explored serves as a straw man proposal to test and knock down proposals as well as prompt discussion on what is achievable.

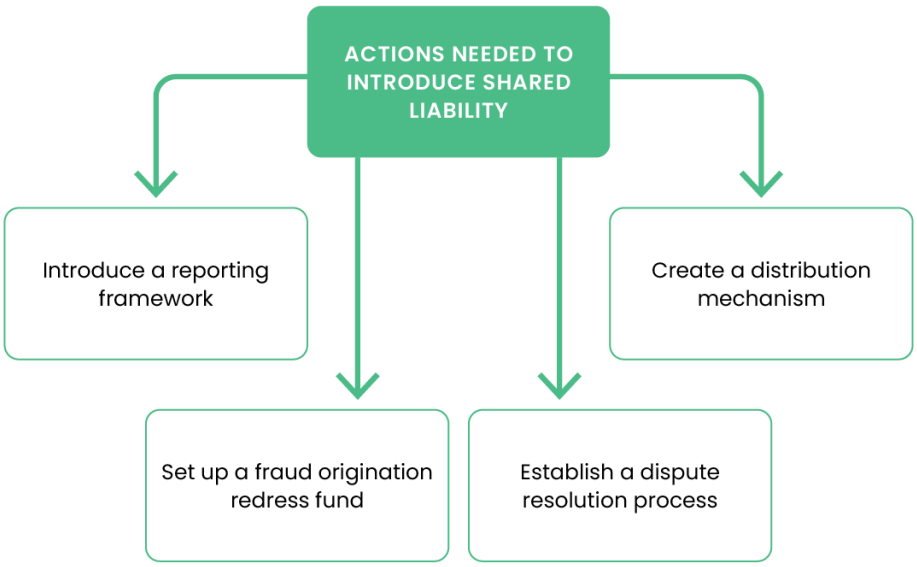
International comparisons

The suggestion to introduce shared liability is not a novel idea. Other jurisdictions have taken or are considering similar measures to tackle payments fraud, having accepted that holding the financial services sector alone responsible for reimbursing victims of fraud to be disproportionate and inefficacious in tackling fraud at source.

Singapore, a key international competitor to the UK in financial services, has announced shared liability between financial institutions, telecommunication operators and consumers for losses incurred from unauthorised payment transactions due to phishing scams.[55] This came into effect in December 2024, following a period of consultation by the Monetary Authority of Singapore (MAS) and the Infocomm Media Development Authority (IMDA).[56] The proposals set out by the MAS and IMDA demonstrates proportionality whereby financial institutions mitigate the risk of seemingly authorised transactions while telcos guard against the risk of subscribers receiving SMSs which facilitate fraudulent transactions. When this responsibility falls short, shared liability to payout fraud victims is required. This is an innovative approach to fraud prevention as Singapore will become one of the few jurisdictions worldwide where mobile network operators must share responsibility with financial institutions, such as banks, and other PSPs.[57]

Similarly, in Australia, the government has plans to introduce legislation where telecommunications companies, social media and banks would face fines and share responsibility in compensating victims, if they failed to adequately prevent the fraud.[58] To effectively introduce this, the legislation would also set out internal dispute resolution mechanisms.[59]

The proposal for shared liability



A number of actions must be taken by the PSR/FCA and Ofcom to introduce shared liability in reimbursing victims of APP scams. This will leverage the National Anti Fraud Centre's (if established) expected work in enabling data sharing and analysis and establishing a safe cross-industry channel for data sharing.

It must be flagged that delivering this proposal will require the Department for Science, Innovation and Technology (DSIT) to amend the Online Safety Act 2023. We first explore proposals for shared liability and subsequently set out high-level views on amendments needed to the Act.

I. Introduce a reporting framework

In consultation with industry, the PSR/FCA should establish a fraud reporting framework where the PSP (either sending or receiving, to whom the victim reported the occurrence of fraud) collects information on where the APP scam originated. This should occur before victims are reimbursed by the sending PSP.

The PSP should also report information on how many pay-outs were made, categorised according to platform source of fraud origination, to the PSR/FCA within a set reporting period. For this to be successful, the PSR/FCA should give a direction that PSPs in-scope of the APP scams mandatory reimbursement framework collect and report this information

in a standard manner. PSPs should then share this information to the PSR/FCA who will subsequently collate and share with Ofcom and if necessary Pay.UK. The rationale for having the PSR/FCA collate and share this data with Ofcom is that it would provide a layer of legitimacy and impartiality over the data shared.

The PSR/FCA should consult with industry on the appropriate reporting period and mechanism to share this data in a way that facilitates cross-industry data sharing and analysis. For example, the role of the RCMS or any equivalent system should be considered in facilitating data reporting. Given the vitality of this to anti-fraud efforts and the interplay with the existing mandatory reimbursement regime, the PSR/FCA, National Anti Fraud Centre (if established) and Pay.UK should be allowed to provide views and support where necessary. Issues and challenges faced by the RCMS and equivalent systems must be considered before they take on expanded and more complex capabilities.[60]

II. Set up a fraud origination redress fund

The PSR/FCA should set up an APP fraud origination redress fund whereby Ofcom-designated "contributing telecommunications and social media platforms" would pay into on aggregate following each reporting period. Ofcom should be given responsibility for this redress fund with the National Anti Fraud Centre (if established) providing support and counsel where needed.

Platforms would pay into this fund according to fraud origination data published by the PSR/FCA.[61] In essence, this would operate like a risk-based economic crime levy proportionate to the scale of fraud originating from the tech platforms.

Other options can however also be considered, such as contributions being made according to a percentage of redistribution that Big Tech firms must pay back to PSPs who have reimbursed victims under the PSR's rules. The level of apportioning of liability can be set by Ofcom in consultation with industry, the PSR/FCA and bodies such as the National Anti Fraud Centre if established.

III. Create a distribution mechanism

A distribution mechanism for payments to PSPs from the fraud origination redress fund should be created. The PSPs could receive funds from the fraud origination redress fund based on the aggregate value of claims they reimbursed in relation to fraud origination from the Big Tech platform in a reporting period. Alternatively, the PSPs could also receive funds based on a percentage of redistribution that Big Tech firms must pay back to PSPs who have reimbursed victims.

The distribution of these funds would be done by a third-party distributor acting at the discretion of Ofcom. There should be full transparency on the terms and conditions that the third-party distributor is subjected to for industry confidence.

IV. Establish a dispute resolution process

Disputes by social media platforms and telecommunication firms about their culpability as sources of fraud origination are expected in relation to some claims. Hence, Ofcom as the overseer of the fraud origination redress fund should establish an internal dispute resolution mechanism between PSPs and Big Tech platforms. This will ensure disputes are resolved and the apportionment of shared liability following each reporting period can be implemented.

If the dispute cannot be resolved internally, it is recommended that the parties should have access to an external dispute resolution scheme. However, this external dispute resolution scheme cannot be overly cumbersome and must not involve lengthy bilateral negotiation, mediation or legal challenge in each case because many small and fledgling FinTech PSPs cannot afford such a model of dispute resolution.

A process that is automated as well as cost and time efficient is necessary to ensure fairness between small PSPs and Big Tech firms.

Measures of success

As outlined in Part 1, the measures of success for shared liability can also include halving payments fraud by 2028 and reduced industry spend on reimbursement. Additionally, success can be judged according to an additional measure.

Reduction in purchase scams by improvements in online peer-to-peer verifications and payments

As discussed above, industry data shows that the vast majority of APP scams that originate on social media platforms relate to purchase scams.[62] Purchase scams often occur when consumers go to online peer-to-peer social media marketplaces such as Facebook Marketplace to purchase goods that never arrive.

These types of fraud are ubiquitous because there are no minimum verification rules on online peer-to-peer marketplaces for both the identity of the seller and their listings. This is also exacerbated by the lack of obligation for these platforms to integrate with secure payment services.

By requiring these Big Tech platforms to share liability for APP scams, there would be an added incentive for these firms to introduce measures that would reduce their spend on paying back PSPs for fraud that originates from their platforms. This could include online peer-to-peer marketplaces taking the following measures:

- Introducing minimum verification rules on online peer-to-peer marketplaces;
- Clamping down on anonymity and making it more difficult to list goods;
- Improving reporting channels for fraud; and
- Integrating with secure payment services.

The benefits of shared liability in reducing purchase scams would also deliver the added benefit of increasing protection to users interacting online. This was a key focus of Ofcom in their consultation on *Protecting people from illegal harms online* where our response argued that proposals should go further by paying more attention to incentivising online peer-to-peer marketplaces to crack down on fraud.[63]

The measures of success outlined are not meant to be exhaustive. Bearing this in mind, trends from some FinTech firms are indicating some movement away from online peer-to-peer marketplaces to telecommunications platforms such as WhatsApp or Telegram. The scale of purchase scams as well as impersonation, investment and romance scams and that the total losses stemming from these might also be in flux.

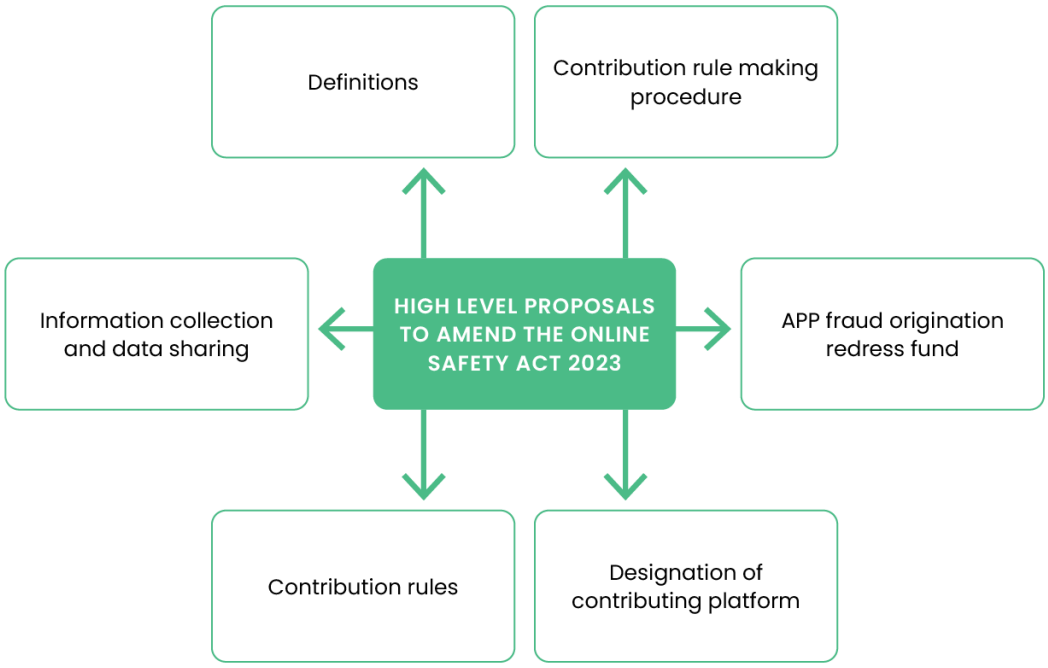
Hence, thought should also be put into how shared liability can provide an impetus to social media and telecommunications firms to better identify and block sophisticated criminals and those who employ complex engineering tactics to prey on victims via their platforms. For example, it has been reported that consumers are being *"duped more easily than ever by cloned websites, deepfake videos and messages impersonating banks or tax authorities"*.[64] More effort to tackle this increased sophistication in fraud can be considered a measure of success for shared liability.

Delivering shared liability: High level outline of amendments needed to the Online Safety Act 2023

The Online Safety Act 2023 as it currently exists requires amendments to facilitate the introduction of shared liability for social media and telecommunications firms.[65] DSIT should consider the amendments to the Act that address:

- The form, manner and period of reporting needed to facilitate shared liability;
- The basis upon which Ofcom will determine the contribution factor (i.e. share of APP scam contribution and repayment);
- Criteria for designation as a "contributing telecommunications and social media platforms";
- Determination and allocation of distribution fees;
- Dispute resolution mechanics; and
- Any other matters Ofcom considers appropriate.

The suggested amendments are explored below.



I. Definitions

Definitions in the Online Safety Act 2023 should be amended include additions related to the APP scams mandatory reimbursement regime (e.g. APP scams, operator, PSP, etc.) as set out by PSR rules pursuant to the powers granted to it under the Financial Services and Markets Act 2023.[66]

Terms that should be defined in the Act to enable Ofcom to deliver shared liability include but are not limited to:

- Fraud reporting framework;
- Contribution amount;
- Contribution factor;
- Contribution rules;
- Redress fund;
- Distributor of funds;
- Distribution fee; and
- Reporting period.

Some further detail on the above terms is explored below.

II. Information collection and data sharing

The Act should set out that the PSR/FCA must impose a relevant requirement, in whatever way and to whatever extent it considers appropriate, on the operator (i.e. Pay.UK as the operator of the Faster Payment Service (FPS)) to:

- Require in-scope PSPs to collect from each claimant information on whether the victim made contact with the perpetrator of the APP fraud on a social media or telecommunications platform in-scope of shared liability, and if so the identity of the platform;
- Set out the content of information to be provided, the form and manner it should be provided and the reporting periods;
- Require this information to be submitted to the designated fraud reporting framework according to requirements set out such as the data points and reporting period; and
- Require the data to be subsequently passed on to Ofcom and relevant authorities.

The PSR/FCA should also issue guidance or amend existing guidance on the meaning of the 'consumer standard of caution' in relation to the APP fraud reimbursement requirement, such that a claimant (except where the claimant has been identified as a vulnerable customer) shall satisfy the 'consumer standard of caution' only if they provide any information requested by PSPs.

III. Contribution rules

The Act should enable Ofcom to make "contribution rules" as to but not limited to:

- The basis upon which Ofcom will determine the contribution factor (i.e. how much Big Tech platforms will contribute to the system and how the contributions will be dispersed to PSPs);
- The criteria to be met in order for Ofcom to designate a regulated user-to-user service as a contributing platform;
- Operation and allocation of the APP fraud origination redress fund;
- Determination and allocation of distribution fees; and
- The scope for bringing and the basis for resolving disputes.

These rules should be drafted in consultation with industry (e.g. regulated user-to-user services and in-scope PSPs), the PSR and FCA, Pay.UK and other relevant authorities (such as the National Anti Fraud Centre if established). Contributing platforms should be required to comply with the rules as published and implemented by Ofcom.

IV. Contribution rule making procedure

Ofcom should be empowered to prepare and issue a draft of the contribution rules that:

- Brings it to the attention of the public; and
- Is accompanied by notice that representations about the proposed contribution rules may be made to Ofcom within a specified period.

V. APP fraud origination redress fund

As noted, Ofcom should consult and determine the contribution factor in accordance with the contribution rules. The Act should allow Ofcom to:

- As an option, determine the contribution amount due from a contributing platform for a reporting period as the aggregate value of the claims related to its platform originated fraud for that period multiplied by the contribution amount; and
- Appoint a distributor to collect and manage the APP fraud origination redress fund and distribution fees.

In relation to payments to the distributor, Ofcom should consult on who should be paying the distributor for its service in an equitable manner. It is recommended that the contributing platforms shall pay to the distributor:

- The contribution amounts calculated and communicated to the contributing platforms by Ofcom. Such payments shall form the "APP fraud origination redress fund"; and
- The distribution fees allocated by Ofcom to the contributing platforms in accordance with the contribution rules.

Following each reporting period, the distributor shall:

- Distribute the value of the APP fraud origination redress fund to PSPs, after the deduction of distribution fees; and

- Pay such portion of the distribution fees as is due to Ofcom.

The portion of APP fraud origination redress fund payable to a PSP could be based on the aggregate value of claims paid by the PSP in relation to platform originated fraud.

VI. Designation as a contributing platform

The Act should allow Ofcom to:

- Designate a provider of regulated user-to-user services (that fall under Category 1 and 2B of the existing Act) as a contributing platform where the provider meets the designation conditions set out in the contribution rules; and
- Publish the designation of a regulated user-to-user service as a contributing platform.

Endnotes

1. Innovate Finance, *FinTech Plan for Government*. See here: *ww2.innovatefinance.com/wp-content/uploads/2024/07/innovate-finance-fintech-plan-for-government.pdf*
2. BBC News, *Warning UK losing £2,300 per minute to fraud.* See here: *www.bbc.co.uk/news/business-65545247*
3. Financial Times, *Is the UK failing victims of fraud?*. See here: *www.ft.com/content/964d2ffc-804c-4016-8c90-814fec68ecb8*
4. 71% of those with annual income of £20,000 or less found that the last fraud they suffered from had a "major" or "moderate" economic consequences. Source here: Social Market Foundation, *Fraudemic: Adding to the evidence base on the scale and impact of fraud on the UK.* See here: *www.smf.co.uk/wp-content/uploads/2023/07/Fraudemic-July-2023-2.pdf*
5. Ibid.
6. Fortune Business Insights, *Fraud Detection and Prevention Market Size.* See here: *www.fortunebusinessinsights.com/industry-reports/fraud-detection-and-prevention-market-100231*
7. HM Treasury, *Financial Services Growth & Competitiveness Strategy: Call for Evidence.* See here: *assets.publishing.service.gov.uk/media/6735f4670b168c11ea82311d/Financial_Services_Growth___Competitveness_Strategy_-_Call_for_Evidence_.pdf*
8. GOV.UK, *Chancellor fires up financial services sector to drive growth.* See here: *www.gov.uk/government/news/chancellor-fires-up-financial-services-sector-to-drive-growth*
9. Innovate Finance and KPMG, *The Roadmap to Open Finance in the UK.* See here: *ww2.innovatefinance.com/wp-content/uploads/2024/04/crt154204a_the-open-finance-roadmap-04.04.2024_v8.pdf*
10. Innovate Finance, *FinTech Plan for Government.* See here: *www.innovatefinance.com/policy-blogs/innovate-finance-fintech-plan-for-government/*

11. HM Government, *Fraud Strategy: Stopping Scams and Protecting the Public.* See here: *assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf*

12. HM Government, *Economic Crime Plan 2, 2023-2026.* See here: *assets.publishing.service.gov.uk/media/642561b02fa8480013ec0f97/6.8300_HO_Economic_Crime_Plan_2_v6_Web.pdf*

13. Payment Systems Regulator, *PSR confirms decision on APP scams reimbursement.* See here: *www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-its-decision-on-app-scams-reimbursement/*

14. Home Office, *Online Fraud Charter.* See here: *assets.publishing.service.gov.uk/media/65688713cc1ec5000d8eef96/Online_Fraud_Charter_2023.pdf*

15. Ofcom, *Creating a safer life online for people in the UK.* See here: *www.ofcom.org.uk/online-safety/illegal-and-harmful-content/safer-life-online-for-people-in-uk#:~:text=Our%20first%20consultation%2C%20due%20in,and%20girls%20by%20Spring%202025.#:~:text=Our%20first%20consultation%2C%20due%20in,and%20girls%20by%20Spring%202025*

16. HM Treasury, *Chancellor fires up financial services sector to drive growth.* See here: *www.gov.uk/government/news/chancellor-fires-up-financial-services-sector-to-drive-growth*

17. Action Fraud: National Fraud & Cyber Crime Reporting Centre. *What we do with your information.* See here: *www.actionfraud.police.uk/what-we-do-with-your-information*

18. City of London Police, *New suppliers appointed for Action Fraud service replacement.* See here: *www.cityoflondon.police.uk/news/city-of-london/news/2023/june/new-suppliers-appointed-for-action-fraud-service-replacement/*

19. Financial Times, *Is the UK failing victims of fraud?.* See here: *www.ft.com/content/964d2ffc-804c-4016-8c90-814fec68ecb8*

20. National Crime Agency, *Fraud.* See here: *www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime*

21. Home Office, *Fraud Strategy: Stopping Scams and Protecting the Public.* See here: *assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf*

22. National Crime Agency, *Ground breaking public private partnership launched to identify criminality using banking data.* See here: *www.nationalcrimeagency.gov.uk/news/ground-breaking-public-private-partnership-launched-to-identify-criminality-using-banking-data*

23. National Crime Agency, *National Economic Crime Centre.* See here: *www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre*

24. HM Government, *Economic Crime Plan 2, 2023-2026.* See here: *assets.publishing.service.gov.uk/media/642561b02fa8480013ec0f97/6.8300_HO_Economic_Crime_Plan_2_v6_Web.pdf*

25. Stop Scams UK, *About*. See here: *stopscamsuk.org.uk/about/*

26. Ibid.

27. Financial Conduct Authority, *Authorised Push Payment Fraud TechSprint.* See here: *www.fca.org.uk/events/authorised-push-payment-fraud-techsprint*

28. Financial Conduct Authority, *Authorised Push Payment Fraud TechSprint Demo Showcase.* See here: *webinars.fca.org.uk/authorised-push-payment-fraud-1/join*

29. Financial Conduct Authority, *Authorised Push Payment synthetic data.* See here: *www.fca.org.uk/firms/digital-sandbox/authorised-push-payment-synthetic-data*

30. Cifas, *National Fraud Database.* See here: *www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/national-fraud-database*

31. Ibid.

32. Joint Regulatory Oversight Committee, Financial Conduct Authority and Payment Systems Regulator, *JROC's proposals for the design of the Future Entity for UK open banking.* See here: *assets.publishing.service.gov.uk/media/66227c3611d9f57e3ba7e58b/JROC_s_proposals_for_the_design_of_the_Future_Entity_for_UK_open_banking.pdf*

33. Pay.UK, *Reimbursement Claims Management System (RCMS).* See here: *www.wearepay.uk/rcms/*

34. GOV.UK, *Chancellor fires up financial services sector to drive growth.* See here: *www.gov.uk/government/news/chancellor-fires-up-financial-services-sector-to-drive-growth*

35. Financial Times, *Is the UK failing victims of fraud?.* See here: *www.ft.com/content/964d2ffc-804c-4016-8c90-814fec68ecb8*

36. PwC and Stop Scams UK, *Future of fraud: A UK view from the 2030s.* See here: *stopscamsuk.org.uk/wp-content/uploads/2024/09/future-of-fraud-august-2024.pdf*

37. Ibid.

38. Bloomberg, *UK's Flagship Fraud System Handles Just 10 Cases Since Launch.* See here: *www.bloomberg.com/news/articles/2025-02-25/uk-s-flagship-fraud-system-handles-just-10-cases-since-launch*

39. Home Office, *Online Fraud Charter.* See here: *assets.publishing.service.gov.uk/media/65688713cc1ec5000d8eef96/Online_Fraud_Charter_2023.pdf*

40. Innovate Finance, *Ofcom consultation "Protecting people from illegal harms online": Innovate Finance response.* See here: *www.innovatefinance.com/policy-blogs/ofcom-consultation-protecting-people-from-illegal-harms-online-innovate-finance-response/*

41. HM Government, *Fraud Strategy: Stopping Scams and Protecting the Public.* See here: *assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf*

42. Financial Times, *Is the UK failing victims of fraud?.* See here: *www.ft.com/content/964d2ffc-804c-4016-8c90-814fec68ecb8*

43. Financial Conduct Authority, *FCA to collect Treasury's economic crime levy (Anti-Money Laundering) from July.* See here: *www.fca.org.uk/news/news-stories/fca-collect-treasurys-economic-crime-levy-anti-money-laundering-july*

44. Payment Systems Regulator, *Unmasking how fraudsters target UK consumers in the digital age.* See here: *www.psr.org.uk/media/u0vnq1ra/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age-dec-2024.pdf*

45. Home Office, *Asset recovery statistical bulletin: financial years ending 2019 to 2024.* See here: *www.gov.uk/government/statistics/asset-recovery-statistics-financial-years-ending-2019-to-2024/asset-recovery-statistical-bulletin-financial-years-ending-2019-to-2024#asset-recovery-incentivisation-scheme-aris* ; CPS, *Proceeds of Crime: Legal Guidance, Proceeds of Crime.* See here: *www.cps.gov.uk/legal-guidance/proceeds-crime*

46. GOV.UK, *Minister of State (Lords Minister): The Rt Hon Lord Hanson of Flint.* See here: *www.gov.uk/government/people/david-hanson*

47. Ibid.

48. GOV.UK, *Prime Minister's Anti-Fraud Champion.* See here: *www.gov.uk/government/people/simon-fell*

49. Innovate Finance, *FinTech Plan for Government.* See here: *ww2.innovatefinance.com/wp-content/uploads/2024/07/innovate-finance-fintech-plan-for-government.pdf*

50. Financial Times, *Is the UK failing victims of fraud?.* See here: *www.ft.com/content/964d2ffc-804c-4016-8c90-814fec68ecb8*

51. HM Government, *Fraud Strategy: Stopping Scams and Protecting the Public.* See here: *assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf*

52. BBC, *Banks warn of big increase in online scams.* See here: *www.bbc.co.uk/news/technology-65486219* ; Financial Times, *Meta singled out by UK financial lobby group over digital scams.* See here: *www.ft.com/content/d0215c7c-90e5-4e53-b5ea-a19140730b21*

53. Innovate Finance, *Ofcom consultation "Protecting people from illegal harms online": Innovate Finance response.* See here: *www.innovatefinance.com/policy-blogs/ofcom-consultation-protecting-people-from-illegal-harms-online-innovate-finance-response/*

54. Ibid.

55. Monetary Authority of Singapore and Infocomm Media Development Authority, *MAS and IMDA Announce Implementation of Shared Responsibility Framework from 16 December 2024.* See here: *www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024*

56. Monetary Authority of Singapore and Infocomm Media Development Authority, *Consultation Paper on Proposed Shared Responsibility Framework.* See here: *www.mas.gov.sg/-/media/mas-media-library/publications/consultations/pd/2023/srf/consultation-paper-on-proposed-shared-responsibility-framework.pdf*

57. The Straits Times, *Shared responsibility framework for online scams to be rolled out in 2024: Alvin Tan.* See here: *www.straitstimes.com/singapore/politics/shared-responsibility-framework-for-online-scams-to-be-rolled-out-in-2024-alvin-tan*

58. The Guardian, *Banks and social media companies to be fined over scams under new Australian laws touted as 'strongest in world'.* See here: *www.theguardian.com/money/2024/nov/07/banks-and-social-media-companies-to-be-fined-over-scams-under-new-australian-laws-touted-as-strongest-in-world*

59. Ibid.

60. Bloomberg, *UK's Flagship Fraud System Handles Just 10 Cases Since Launch.* See here: *www.bloomberg.com/news/articles/2025-02-25/uk-s-flagship-fraud-system-handles-just-10-cases-since-launch*

61. Payment Systems Regulator, *Unmasking how fraudsters target UK consumers in the digital age.* See here: *www.psr.org.uk/media/u0vnq1ra/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age-dec-2024.pdf*

62. Innovate Finance, *Ofcom consultation "Protecting people from illegal harms online": Innovate Finance response.* See here: *www.innovatefinance.com/policy-blogs/ofcom-consultation-protecting-people-from-illegal-harms-online-innovate-finance-response/*

63. Ibid. ; Ofcom, *Consultation: Protecting people from illegal harms online.* See here: *www.ofcom.org.uk/online-safety/illegal-and-harmful-content/protecting-people-from-illegal-content-online/*

64. Financial Times, *Is the UK failing victims of fraud?.* See here: *www.ft.com/content/964d2ffc-804c-4016-8c90-814fec68ecb8*

65. Legislation.gov.uk, *Online Safety Act 2023.* See here: *www.legislation.gov.uk/ukpga/2023/50*

66. Legislation.gov.uk, *Section 72, Financial Services and Markets Act 2023.* See here: *www.legislation.gov.uk/ukpga/2023/29/section/72*

Get in Touch

Contributors

Adam Jackson

Chief Strategy Officer

adam@innovatefinance.com

Christopher Foo

Senior International Policy Associate

christopher@innovatefinance.com

INNOVATE FINANCE

Innovate Finance policy team:

policy@innovatefinance.com

About Innovate Finance

Innovate Finance is the independent industry body that represents and advances the global FinTech community in the UK. Our mission is to accelerate the UK's leading role in the financial services sector by directly supporting the next generation of technology-led innovators. When engaging the government and regulators, we aim to reflect the UK FinTech ecosystem and specifically the needs of start-ups, scale-ups and high growth enterprises.

The UK FinTech sector encompasses businesses from seed-stage start-ups to global financial institutions, illustrating the change that is occurring across the financial services industry. Since its inception in the era following the Global Financial Crisis of 2008, FinTech has been synonymous with delivering transparency, innovation and inclusivity to financial services. As well as creating new businesses and new jobs, it has fundamentally changed the way in which consumers and businesses are able to access finance.

Our membership base is diverse across FinTech and financial services including but not limited to challenger banks, payments firms, electronic money institutions, consumer credit providers, credit information providers, alternative credit rating agencies, wallet providers, personal finance apps, RegTech firms and digital asset firms.


INNOVATE/FINANCE