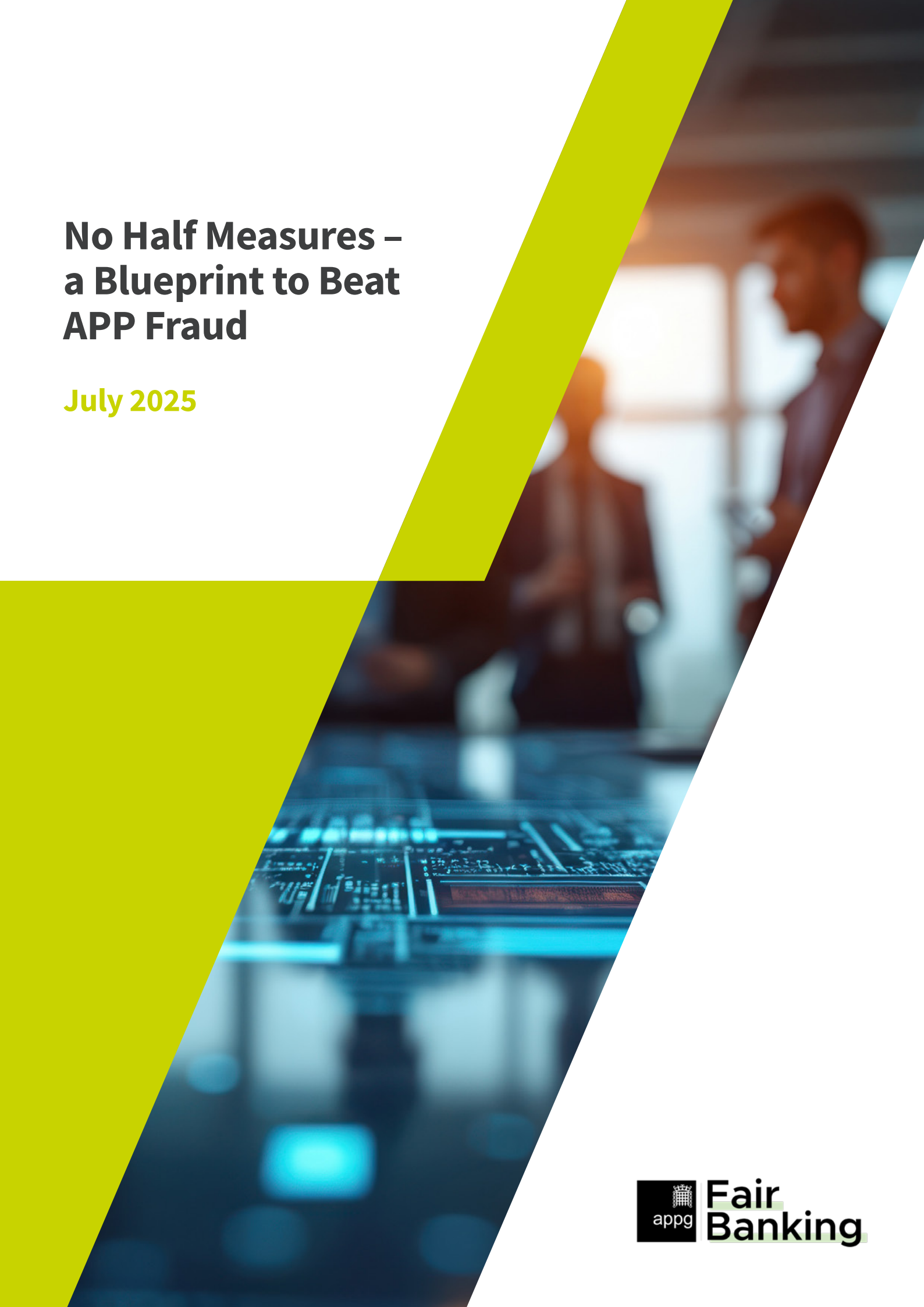
No Half Measures – a Blueprint to Beat APP Fraud

July 2025



appg Fair Banking

About the APPG on Fair Banking

The APPG is a cross-party group with members from the House of Commons and the House of Lords which puts forward policy recommendations to Government that encourage a fairer financial system to level the playing field between businesses, consumers and their lenders. The Group acts as a forum and focal point for individuals, SMEs and the financial services industry to deliver reforms in their long-term interest.

About Tide

Tide is a business financial platform serving the diverse needs of SMEs, by providing them with products catered to alleviating their admin and bureaucratic pains. Tide's app houses invoicing, accounting, subscription plans, loans, cards, point of sale card readers and much more. Launched in the UK in 2017, in India in 2022, in Germany in 2024, it now counts 1.4m SMEs as customers (known as members). The scale of its growth is in the numbers; it now has more than 2000 employees in the UK, India, Bulgaria, Germany and Lithuania, and is focussed on its next international market, likely to be in Europe.

About the author

Benjamin Barnett, Senior Research and Policy Advisor, The Athena Foundation

Benjamin has a background in sustainable finance, having written extensively on the development of sustainable finance regulation around the world. Since joining the Athena Foundation, secretariat for the APPG on Fair Banking and the APPG on Sustainable Finance, Benjamin now works on policy issues related to economic crime and sustainable finance in the UK. He is also the co-author of the recently published report, 'Clean Foundations for Growth', from the APPG on Anti-Corruption and Responsible Tax and the APPG on Fair Banking.

Research Support – Alice Forster, Parliamentary Researcher, The Athena Foundation

Produced with the support of Tide.

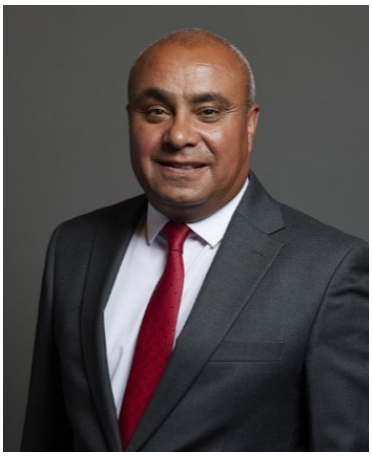
Disclaimer

Table of contents

Glossary of terms

APP Fraud	*Authorised Push Payment Fraud:* A type of scam where individuals or businesses are tricked sending money to a fraudster.
CHAPS	*Clearing House Automated Payment System:* UK payment system used for high-value, same-day transfers.
CRM	*Contingent Reimbursement Model:* Voluntary scheme of reimbursement, in place prior to the implementation of the MRR; provided partial reimbursement.
Faster Payments	Service that allows near-instant transfers between banks' customer accounts.
FATF	*Financial Action Task Force:* An intergovernmental body that's sets global standards for fighting money laundering.
FCA	*Financial Conduct Authority:* UK's financial regulatory body responsible for conduct and prudential regulation of financial services firms.
FOS	*Financial Ombudsman Service:* An independent body that resolves disputes between consumers and financial service providers. Those with APP fraud losses over £85k that aren't covered by the MRR can seek compensation here.
FSCS	*Financial Services Compensation Scheme:* UK scheme that protects consumers when financial firms fail, offering compensation at a set limit.
GDPR	*General Data Protection Regulation:* The UK's data protection and privacy law.
ICO	*Information Commissioner's Office:* The UK's independent authority for data protection.
KYC	*Know Your Customer:* A process financial institutions use to verify the identity of their customers.
MRR	*Mandatory Reimbursement Requirement:* Regulation, introduced by the PSR, requiring PSPs to reimburse victims of APP fraud with losses of £85k or less.
NCA	*National Crime Agency:* The leading agency tackling serious and organised crime in the UK, including fraud.
PSP	*Payment Service Provider:* A company that facilitates the sending/receiving of payments.
PSR	*Payment Systems Regulator:* UK regulator responsible for payment systems and implementing the MRR.

Foreword



David Burton-Sampson MP, Co-Chair, APPG on Fair Banking

The UK is facing an APP fraud epidemic. Citizens and businesses are under attack from fraudsters seeking to manipulate them into voluntarily transferring legitimate wealth into the hands of criminals. Fraud is now the most prevalent crime against individuals in the UK, and a recent APPG on Fair Banking Report estimated the annual cost of APP fraud at £3.3bn. These costs are unpalatable at any time, never mind with an economy under pressure and growth at the forefront of the government's agenda. Fraud is also a recognised threat to national security and has profound social and psychological impacts on the victims of fraud.

The UK has emerged from the 'lost decade of counter-fraud' and has the opportunity to lead the fight against APP fraud. The 2023 Fraud Strategy was encouraging, leading to some important advancements, including a landmark bank on SIM farms. The recently introduced mandatory reimbursement requirement is also a valuable step protecting consumers and incentivising prevention on the part of payments service providers.

Despite progress, the fraudsters are still winning. APP fraud remains rampant and continues to evolve. AI is transforming fraud, with criminals increasingly able to tailor to their target and utilise deepfake technology to engender trust. Our response must be equally innovative and agile.

There can be no half measures in the fight against fraud. The announced updated Fraud Strategy is much welcomed and represents a valuable opportunity to commit to a holistic approach to combatting fraud.

70% of APP Fraud originates online, and we must do more to include social media companies in a collective counter-fraud response. Key to this is enabling effective cross-sector data and intelligence sharing.

Despite notable successes, more must be done to equip law enforcement to fight APP fraud. Equally, as 70% of fraud includes an international element, the UK must be at the heart of the global response. Fraud has also become incorporated within organised criminal gangs, requiring cross-border, targeted action to strike the arteries of fraud globally.

We must also ensure that the British people are equipped with the information, skills and tools to recognise and protect themselves from scams. A resilient and informed population is a protected one.

We have a fight on our hands. This report outlines a realistic, cross-party blueprint for tackling APP fraud in the UK. We can win the war against fraudsters, but to do so requires ambitious, collective and coordinated action.

Executive Summary

The purpose of this report is two-fold:

1. To analyse the Mandatory Reimbursement Requirement (MRR) from the Payment Systems Regulator (PSR) requiring Payment Service Providers (PSPs) to reimburse customers who are victims of fraud that takes place on their platform.
2. Beyond the MRR, to understand what measures should be prioritised in the updated Fraud Strategy in order to address the problem of APP fraud in a way which is comprehensive, collaborative, and fair.

Context

The UK is emerging from a long winter of counter fraud. During the 2010s, known as the 'lost decade of counter-fraud', scammers gained a foothold in the UK. Among the most pernicious types of fraud to have exploded during this period is Authorised Push Payment (APP) fraud, in which individuals and organisations are manipulated and deceived into sending criminals money.

A new era of counter-fraud

In the past years, the Government has made positive strides, with the 2023 Fraud Strategy marking a sea change in the fight against fraud. It set the stage for what has been described as 'arguably the most polarising policy initiative in the history of the UK counter-fraud industry'. In October 2024, the PSR introduced a Mandatory Reimbursement Requirement, requiring PSPs to reimburse victims of fraud which take place on their platforms.

It is still early days for the regulation, and assessing overall impact will take time. An independent one-year review will take place to assess the impact of the MRR, as well as assessing the PSR's wider policy approach to APP fraud. From conversations the APPG has had with industry stakeholders in interviews and series of roundtables, several themes emerged which should be key focus areas for the independent review and the PSR moving forward (please see Recommendation Longlist for full details):

- **The £85,000 limit:** Investigate whether the £85,000 reimbursement threshold appropriately balances consumer protection and costs to PSPs, especially given early data showing that victims in the first 3 months of the regulation only got back 86% of losses by value.
- **Fraud prevention efforts:** Examine whether PSPs are investing adequately in fraud detection and prevention, and if the current incentives and standards are sufficient or require further standardisation and guidance.

- **Consistency in implementation:** Clarify and address ambiguities in applying consumer standards of caution and distinguishing fraud from civil disputes to ensure consistent treatment of cases by PSPs. Engagement with the Financial Ombudsman Service (FOS) is essential on this point.
- **Burden on PSPs:** Assess the full impact of the MRR's reimbursement and compliance costs on PSPs, particularly smaller providers, and evaluate whether these costs negatively affect competition.
- **Data sharing:** Consider the effectiveness of current data-sharing arrangements between PSPs, and whether mandatory, statutory-level data sharing should be implemented.
- **Consumer awareness and experience:** Undertake a consumer survey to evaluate whether the MRR has increased friction between customers and PSPs, understand consumer experience and customer awareness about the MRR have impacted consumer behaviours and attitudes towards reimbursement and fraud prevention.
- **Shifting fraud trends:** Analyse whether the MRR is inadvertently pushing fraudsters to other fraud types and channels, including unauthorised fraud and international transactions, and assess whether further regulatory steps may be necessary.

The PSR issued the Invitation to Tender (ITT) for the independent review in early June, in which they set out a minimum scope of the work. As the work commences later this year, the PSR have confirmed that the APPG's report – and its suggestions on scope of the review – will be passed onto the independent party leading the evaluation, who can refine the scope if they feel it is appropriate

The MRR can be a powerful tool for protecting consumers from the worst economic impacts of fraud, but it does not solve the problem of fraud, and alone is at best insufficient, and at worst unfair. Financial institutions will have a crucial, ongoing role to play in the fight against APP fraud. Nonetheless, viewing financial institutions as the beginning and end of fraud prevention and protection places an excessive burden on them, whilst also failing to comprehensively tackle the issue of fraud in all its complexity. The ultimate success of the MRR is contingent on what comes next, and where is sits within a broader approach to beating APP fraud.

APP fraud is a multi-faceted problem which requires a multi-faceted solution, and the Government's announced update to the Fraud Strategy represents a crucial opportunity to prioritise a holistic 'whole-of-ecosystem' approach which balances approaches, responsibilities and liabilities, and utilising every tool in the Government's arsenal to tackle fraud in the UK and internationally. The following areas should be prioritised in the Fraud Strategy (see Recommendation Longlist for full details).

1. **Close the gaps in reimbursement and maintaining protections –** pending the evaluation of the one-year review, consider expanding reimbursement rules to cover cryptocurrency and international transfers. In absence of greater regulation, the FOS' 'fair and reasonable' remit must be maintained to assess cases which fall outside of the MRR.

2. **Ensure a renewed focus in understanding the impact of fraud on businesses,** and what can be done to better protect businesses from fraud and support them in prevention efforts.

3. **Place prevention at the strategic heart of counter-fraud** by leveraging the whole ecosystem. Ensure social media and telecommunication companies play their part through the introduction of a 'tech levy', scoping the possibility for cost sharing on reimbursement, placing the Online Fraud Charter on a statutory footing, and bringing forward the implementation of the Online Safety Act.

4. **Enable cross sector data sharing** by providing a centralised data sharing platform and issuing clear and practical guidance on how to confidently share data in compliance with GDPR.

5. **Provide an effective deterrent to fraud** by reforming fraud policing and the criminal justice system. Provide multi-year, ring-fenced core funding for policing, boosted by the establishment of an Economic Crime Fighting Fund. Streamline roles and responsibilities in policing and prioritise 'quality' interventions which target the online and upstream arteries of fraud, rather than mass arrests and prosecutions.

6. **Reform the criminal justice system** so that it is fit to handle 21st century crime, revising sentencing guidelines to reflect the societal harms of fraud and expanding dedicated Economic Crime Courts.

7. **Lead the international response to the global threat of fraud,** working cross-border on targeted enforcement and intelligence sharing. Ensure the UK works closely with China to disrupt centres of fraud in East Asia, and leads a global coalition of the willing in the fight against fraud.

8. **End the UKs role as an enabler of fraud** by focussing on the onward proceeds of fraud and the role of the UK and its overseas territories in enabling money laundering.

9. **Foster a fraud resilient population** through an 'education from all angles' approach, whilst improving victim support and supporting those most vulnerable to APP fraud.

There can be no half measures in the fight against APP fraud. The recommendations in this report would form a holistic strategy that is:

1. **Ambitious –** setting bold goals, expanding reimbursement, prevention, data-sharing, enforcement and education at scale.
2. **Collective –** enlisting every stakeholder – from government, regulators, and law enforcement to financial institutions, crypto firms, tech platforms and the public.
3. **Collaborative –** breaking down silos, fostering cross-sector and international partnerships to share intelligence, coordinate operations and align incentives.
4. **Comprehensive –** covering the full fraud lifecycle – prevention, detection, redress, deterrence and victim support, and using every tool and tactic to achieve them.
5. **Fair –** distributing obligations and liabilities proportionately, ensuring no group bears an undue burden.
6. **Integrated –** ensuring APP fraud measures are viewed as one manifestation of a broader problem, integrated within the broader Fraud Strategy, Economic Crime Plan, international efforts, whilst recognising cross-departmental dependencies.
7. **Agile –** equipping the collective response and building in mechanisms for rapid adaptation to emerging threats and new technologies, whilst investing in and adopting leading-edge technologies to stay ahead of the curve.

The UK can lead the fight against APP fraud. The recommendations in this report provide the blueprint for the Government to do so.

Introduction – the seven pillars of a holistic strategy to beat APP fraud

Fraud is a scourge on the British people, decimating personal and public finances, destroying trust, and causing untold mental and emotional distress. One of the most pernicious types of fraud is Authorised Push Payment fraud (APP fraud). In these frauds, individuals and organisations are tricked into voluntarily sending money to a fraudster's account. Fraudsters manipulate in order to steal billions from the public every year, with a recent report from the APPG on Fair Banking estimating the cost at approximately £3 billion annually. Additionally, at a time where economic growth is front of mind for the Government, haemorrhaging billions to fraud undermines broader efforts.

No one is immune from APP fraud, and individuals become targets simply by going about their daily lives. 73% of adults have been targeted by APP fraud, with 35% losing money to fraud.

The tide is changing, however. In the UK, pioneering measures are being taken by Government and industry to tackle the growing and evolving threat of APP fraud. At the forefront of this are the new Reimbursement Rules from the Payment Systems Regulator with Payment Service Providers (PSPs) now required to reimburse the victims of APP fraud that takes place on their platforms.

Reforms such as these are bold and untested and being out in front on APP fraud reimbursement comes with risks. Entering the unknown inevitably brings with it unforeseen consequences, with certain players bearing a greater share of the burden, at least in the short-term. The new reimbursement rules have been described as 'arguably the most polarising policy initiative in the history of the UK counter-fraud industry', and the eyes of countries around the world are on the UK.

At the independent one-year review of the scheme, it is crucial that the right questions are asked, and the right data gathered, to understand the full range of direct and indirect effects. The review will also go beyond reimbursement, looking at the PSR's wider policy programme to ensure a holistic assessment of APP fraud policy effectiveness.

Fraudsters target vulnerabilities in individuals, organisations and systems as they emerge. They use advanced social engineering and manipulation, along with new and evolving technologies, allowing for a greater range of tactics, and more tailored attacks. In addition, the perception of fraudsters as individuals acting alone or in small scale operations is no longer reality. The fraud epidemic, including APP fraud has been turbocharged by organised criminal gangs, attracted by the 'low-risk, high-reward' business model of online fraud. Online fraud now compares in size and scope to the illegal drug industry.

This means that the UK's response to fraud cannot be static. Whilst the steps taken to date are important, tackling APP fraud cannot be boiled down to reimbursement, or even advanced prevention systems within payment service providers.

> *Reimbursement must be part of an agile, integrated approach that builds awareness and resilience among the population, understands the full scale and nature of the problems through data-sharing, cuts off the tools, loopholes and enablers utilised by fraudsters, and targets large-scale criminal operations at source via international cooperation.*

The Government has appointed Lord Hanson as the UK's first dedicated Fraud Minister. Lord Hanson and the Joint Fraud Taskforce have been tasked with updating the UK's Fraud Strategy, due for release towards the end of 2025. This represents a crucial opportunity to place a holistic approach to fraud, including APP fraud, at the heart of the UK's counter-fraud strategy.

This research is therefore split into two parts:

1. The first section examines the MRR itself, analysing early indications as to its efficacy and consequences, with an eye to what needs to be answered at the one-year review later this year.
2. The second section will zoom out to see how the MRR should fit within a broader spectrum of APP fraud reforms and initiatives, making recommendations for the UK's updated Fraud Strategy.

To do this, we brought together stakeholders from across the counter-fraud ecosystem in a series of roundtables to discuss the present and future of tackling APP fraud in the UK. The following analysis draws on voices from consumer groups, regulators, financial institutions and industry associations, representing a broad-church of perspectives on the wicked problem of APP fraud. Ultimately, addressing the fraud epidemic must be a collaborative endeavour with collective buy-in. This report lays the blueprint for such an approach.

'The Lost Decade of Counter-Fraud'

The introduction of the new reimbursement rules (from this point on referred to as the 'Mandatory Reimbursement Requirement' or 'MRR') comes off the back of what has been described as the 'lost decade' in counter-fraud. The 2010s represented a period of stagnation in the Government's counter-fraud efforts, which coalesced with technological and societal changes which transformed the scale and the nature of fraud. In this period, while the Government's response languished, fraudsters gained ground. As financial institutions focussed more on unauthorised fraud, this left the customer as the vulnerable link in the chain.

APP fraud in the UK has been fuelled by multiple, interconnected factors.

1. **English speaking:** The widespread use of English in the UK makes it an ideal target for APP fraud, as fraudsters can easily impersonate trusted entities and effectively communicate deceptive messages to a large audience.
2. **Faster payments:** Faster payments systems, rolled out in the UK in 2008, provide an ideal environment for fraudsters. Near-instant, irrevocable transfers fuel APP fraud – 98% of fraud by volume in 2022 used Faster Payments.
3. **Evolutions in technology:** In 2023, 80% of APP frauds started online, with 54% originating on Meta Platforms. Social media platforms provide fraudsters with high anonymity and unparalleled access to a bottomless supply of potential victims, as well as opening new methods and avenues to creatively engineer fraud.
4. **Covid-19:** The pandemic drove people online, spurring adoption of online banking and the growth of new fraud types – investment scams rose 32% in 2020 and romance scams by 38%, accelerating calls for stricter fraud regulation.

Britain – the fraud capital of the world

The result of these trends occurring across the lost decade of the 2010s and into this decade is a nation under siege by fraudsters. According to the National Crime Agency (NCA), fraud is now the most likely crime for someone in the UK to experience, accounting for over 40% of crime in England and Wales.

The UK, off the back of these trends, at the beginning of the 2020s had become known as the 'scam capital of the world' – the global epicentre of fraud attacks. Faster-payments, an under-funded approach to fraud policing, plus the use of English – has made the UK an ideal global test bed for fraud, with a Reuters article going so far as to say that APP fraud scams 'are proliferating globally after having started off as a largely UK phenomenon.'

The criminals are winning, and are growing in confidence, sophistication, viciousness and audacity.

The rest of the world find itself in a similar position, battling to catch up with proliferation of scams. Other countries are experimenting with approaches to counter-fraud, which the UK must keep a close eye on for its own evolving approach.

Australia's Scam Prevention Framework

Australians lost approximately AUD 3.1 billion to scams in 2022 – an increase of 80% from the previous year. This prompted Australia to take a whole-of-ecosystem stance by enacting the world-first Scams Prevention Framework in early 2025. The framework mandates that banks, telcos, and digital platforms actively detect, disrupt, and report scam activities – or face fines of up to AUD 50 million. A National Anti Scam Centre has been established to coordinate intelligence-sharing and sector-wide fraud prevention.

Singapore's Shared Responsibility Framework

Scams in Singapore have surged in recent years. In 2023, over 45,000 cases were reported with losses exceeding S$650 million, representing a increase from just 5,300 cases in 2016. Singapore has adopted a multi-pronged Shared Responsibility Framework – placing duties on financial institutions and telecom operators to implement real-time fraud surveillance, kill-switches, cooling off periods, and scam filtering, with expectations to compensate victims if these duties are breached. These structural measures are bolstered by authorities like the Anti Scam Command and IMDA's proactive campaigns.

The problem of APP fraud is unignorable. Multiple players have a role to play, including consumers, financial institutions, social media and law enforcement, but deciding how to divide responsibilities, incentives and disincentives effectively and fairly is no easy task.

> *Ambitious reform is required, necessitating bold steps into the regulatory unknown.*

No half measures – the seven pillars of counter fraud

Based off extensive conversations with stakeholders from across the counter-fraud ecosystem, it is clear that a holistic solution is necessary to address APP fraud in the UK. There can be no half measures in the fight against fraud. A 'no half measures' approach to counter-fraud can be boiled down to seven key pillars that should inform the UK Government's approach:

1. **Ambitious** – Any strategy and contained reforms should be ambitious in their aims and methods.
2. **Collective** – All actors with a role to play in protecting consumers and preventing fraud should be included in the Government's approach to counter-fraud. The Government must incentivise, enable and if necessary, mandate participation, especially for those who play a part in enabling fraud.
3. **Collaborative** – A problem shared is a problem halved. Any response to fraud cannot be siloed. Rather, it should be collaborative. It is the Government's role to itself collaborate across the counter-fraud ecosystem, whilst coordinating and facilitating collaboration between and within stakeholder groups.
4. **Comprehensive** – There is no proof-of-concept on how to beat APP fraud, and therefore the government must be exhaustive in terms of its tools, tactics and targets.
5. **Fair** – The response should not place undue and disproportionate burdens on particular stakeholders in the counter-fraud ecosystem. A long-term strategy should be fair and balanced in order to not generate adverse unintended consequences.
6. **Integrated** – Each individual measure and reform should be integrated within a broader, coordinated strategy to beat APP fraud. Moreover, the approach to APP fraud should be effectively integrated within a broader strategy to fight fraud, so as not to push the problem elsewhere. Scams, including but not limited to APP fraud broadly cost UK people £11.4 billion, which is itself a part of a broader problem costing individuals, the private sector, and the public sector an estimated £219 billion.
7. **Agile** – The goalposts are constantly moving in the fight against fraud. Any response must be agile to new and emerging threats, including the use of new technologies.

These seven pillars form the basis for a strong, balanced, and holistic approach to combatting APP fraud.

With the introduction of a much welcome Fraud Strategy in 2023, the UK emerged from the long winter of counter-fraud and entered a new era. One measure to come out of this is the Mandatory Reimbursement Requirement (MRR), which came into force in October 2024. The MRR is untested and controversial, requiring assessment on two fronts. Firstly, whether it is effective in achieving its stated aims and what consequences it may have, and secondly, how it should fit within the UK's broader approach to counter-fraud.

Section 1

Assessing the Mandatory Reimbursement Requirement

The MRR did not emerge from a blank canvas. A Which? 2016 super complaint argued for financial institutions to face increased liability when it came to APP fraud, and in 2019 the Contingent Reimbursement Model (CRM) was introduced.

An experiment in PSP-led reimbursement – the Contingent Reimbursement Model

The CRM was a voluntary regime including 10 leading banks, covering approximately 90% of payments. The CRM led to improvements in the reimbursement rate. Pre-code, before any industry framework, the industry average reimbursement rate by value was just 19% in the first half of 2019. By 2023, reimbursement value rose to 67% and APP-fraud growth decelerated from 45% year-on-year in 2019 to 12% in 2023. The CRM had issues as well, however, with uneven protection due to its voluntary nature, inconsistent standards and practices, and limited enforcement powers on the part of the Lending Standards Board, who oversaw the scheme.

The Mandatory Reimbursement Requirement

Introduced by the Payment Systems Regulator (PSR) and replacing the CRM, the MRR is a legally binding framework designed to ensure victims of APP Fraud are reimbursed – quickly and consistently – while driving the industry to prevent fraud in the first place. The regulation has some key features which are intended to drive these goals:

Key Features at a Glance

Scope & Obligations

Covers all Faster Payments and CHAPS transactions sent and received in the UK by direct or indirect PSP participants.

PSPs must reimburse claimants who meet the Consumer Standard of Caution in almost all cases.

Timelines & Process

5 business days for initial decision and reimbursement (if approved).

35 business days maximum for final resolution, with “stop-the-clock” pauses only for fact-gathering.

Financial Framework

£85,000 cap per claim.

Optional customer excess up to £100 (cannot be applied to claims made by vulnerable customers).

Innovative 50/50 cost-share between sending and receiving PSPs to incentivise prevention.

Exceptions & Protections

Gross Negligence carve-out: refusal only for very serious customer failings.

Malicious Fraud: no reimbursement if the customer is complicit.

Data Reporting & Enforcement

Monthly reporting to Pay.UK under its Compliance Data Reporting Standards.

PSR can impose fines, directions and other sanctions for non-compliance.

This section will not be a comprehensive review of the effectiveness of the MRR, as an in-depth one-year review of the regulation is planned and will have the benefit of extensive data.

From conversations between the APPG and expert stakeholders from across the counter-fraud landscape, as well as early data, we can see signs as to whether the MRR is having its intended impact, as well as teething problems and potential unintended consequences. These can inform some areas for the one-year review to examine.

Perhaps most importantly, however, exploring the unintended, and in some ways inbuilt consequences of the MRR, can help inform the UK's wider approach to addressing APP fraud as part of the Government's updated Fraud Strategy.

Early indications

The MRR was only brought into force on October 7th 2024, meaning that at present there is sparse data to assess the impact. The APPG has received Pay.UK data from the PSR from the period 7th October to 31st December 2024, covering the first three months since the introduction of the MRR. Early signs suggest that the MRR is having its desired effect.

Reimbursement is going up

Data from the first three months of the policy shows that APP fraud victims got back 86% (value) of their money, totalling around £27m. Although there cannot be a direct comparison due to the significant changes in the definition of an APP, UK Finance data from 2023 reports that only 68% for consumers were reimbursed. In addition, 14% of APP fraud claims were made by consumers that are vulnerable, equating to £7 million, indicating an improvement brought about via additional protections for the most vulnerable.

Broader coverage and better collaboration

There were 60 PSPs that received a claim and reimbursed victims of APP fraud within the first three months of the policy, marking a change in comparison to the CRM (only 10 signatories). There has also been better collaboration between PSPs under the 50/50 split model – most claims (86%) were reported by the sending PSP to the receiving PSP within 2 business hours of the consumer raising the claim. Additionally, 84% of claims were closed within 5 business days.

Instances of APP fraud

Despite an initial fear that reported fraud cases would spike with the introduction of mandatory reimbursement, this has not been seen.

There were around 46,000 claims from consumers in the first three months. UK Finance's annual fraud report 2024 reported 232k cases of APP fraud in 2023, which equates to 58k cases across an average three-month period in 2023, although direct comparisons are not possible between these figures. However, it is possible that some of this data arises from fraud which took place before the introduction of the MRR, and it is unclear as to the level of consumer awareness of the new reimbursement rules, which potentially impact this figure. Claims are increasing month on month so it will be interesting to see where the levels are at the one-year review.

Customer caution

There was concern of increased 'moral hazard', with consumers becoming more careless – or even reckless, due to mandatory reimbursement. However, just 2% of total claims were rejected in the first three months of the policy because consumer standard of caution was not met. Again, understanding consumer awareness of the policy change is essential in understanding consumer behaviour, which should be a focus of the independent review.

Increased investment in prevention

In conversations the APPG has had with industry, it has been a consistent feature that the MRR has incentivised prevention, with many firms investing heavily in technology, systems and customer awareness.

Areas for further investigation

The £85,000 reimbursement limit

One of the topics of greatest controversy surrounding the MRR was the reduction in reimbursement limit from £415,000 to £85,000. Inevitably, whether the level has been set appropriately will be central to the one-year review, as whilst it moderates costs on PSPs, it also exposes consumers to liability above a certain threshold.

Before the MRR came into effect, the PSR estimated that 99% of payments by volume and 90% by value would be in scope of the reimbursement limit of £85,000. Early data suggests that APP fraud victims got back 86% (value) of their money, totalling around £27m. There has therefore been an early 4% increase in the amount not reimbursed compared to what was projected. 14% falling outside of the MRR's scope is not insignificant and requires further investigation as to the nature of these cases. It is also not yet clear what proportion of this 14% is also due to the £100 excess, rather than fraud above the £85,000 limit.

Those who are defrauded above the limit are not left totally without recourse. They can take their case to the Financial Ombudsman Service (FOS) – it is essential that the independent review engages with the FOS to understand whether there is a need for mandatory reimbursement above that level.

Keeping a close eye on prevention

The MRR was designed to incentivise investment in improved fraud detection and prevention by PSPs. The PSR has not been prescriptive however in how PSPs should approach fraud prevention and detection. This was a point that was raised by Emma Lovell of the Lending Standards Board, who oversaw the voluntary CRM code, who wrote, "Perhaps the key difference between the Code and the new framework is the approach to prevention and detection. Although the PSR expects its reimbursement requirements to spur individual financial providers to act on prevention and detection, there will be no binding, sector-wide obligation to do so."

The Lending Standards Board have said they will develop a new Standard focussed on best practice for preventing and detecting APP fraud, but this is yet to be published. The independent review should examine the measures taken by PSPs and work with the LSB to examine whether there is a need for further standardisation, support and information sharing regarding prevention and detection.

Consistent implementation is key

Despite the clarity and ambition of the MRR, there remain areas where the lack of precedent leaves room for interpretation, which should be carefully examined in the one-year review. For example, the customer standard of caution which requires 'gross negligence' on the part of the customer, although intended to be a high bar, can be contested as it is not exactly clear what behaviour would qualify.

> *Kathryn Westmore, Senior Research Fellow at RUSI, is quoted in the FT saying, "There are quite a lot of get-outs for the banks… If you ignore five pop-up alerts, is that gross negligence?".*

Similarly, the line between fraud and 'civil dispute' is unclear, with the FT hearing a case of someone who put six figures into an investment scheme that was revealed to be a fraud, but his bank deemed this a civil dispute, or an investment gone wrong, rather than APP fraud.

The Financial Ombudsman Service (FOS) is tasked with arbitrating disputes between the consumer and their PSP, and it is essential that the independent review engages with the FOS regarding disputes it has handled to understand whether further action is needed to ensure consistency in how the consumer standard of caution and the delineation between fraud and civil dispute are implemented.

Large and uneven burden on PSPs

The PSR recognises that there are significant costs for PSPs under the new regulation. These costs include the amount reimbursed, increased investment in fraud prevention and detection, and additional costs.

In conversations the APPG has had with PSR representatives, they emphasised that to their knowledge the reimbursement requirements had not driven any market exits to date. Nonetheless, the burden inevitably is significant for some PSPs, and logically this would be felt more relatively by smaller PSPs.

Since this feature is in-built and considered in the cost-benefit analysis undertaken by the PSR, it is unlikely that changes will be made to lessen the burden on PSPs. Even if there were leniencies for smaller market participants, they would be at a competitive disadvantage, as reimbursement would become a point of difference for larger PSPs to attract customers.

As prevention improves, the cost of reimbursement should decrease in line with instances of fraud, but within the bounds of the MRR itself, there is only so much that can be done to soften this burden.

The PSR's policy brings an estimated 1,500 additional PSPs into scope and questions have been asked whether increased costs to banks could, in an extreme scenario, lead to an end to the free banking model. The independent review should therefore endeavour to understand the full impact of additional costs on PSPs, the impact it has had on competition, and potential further consequences. This understanding is key in gauging the need for further reform.

Data and intelligence sharing between PSPs

One of the core focus areas of the one-year review should be data sharing. The PSR has called in the past for "improved intelligence sharing to spot fraudulent transactions and stop them from happening", tasking industry with pioneering approaches to sharing data. The PSR stopped short, however, of mandating full-market data-sharing.

Data sharing between PSPs is fragmented and in some areas absent. According to the Payments Association "While organisations such as Pay.UK and Cifas facilitate a level of data sharing, many smaller PSPs are often excluded from these efforts. Despite driving much of the innovation in the payments industry, these smaller firms suffer disproportionately from financial crime losses. Their lack of inclusion in broader data-sharing frameworks leaves them more vulnerable to fraud."

In conversations between the APPG and representatives of the PSR, they say that plans are being developed to enhance firm-to-firm data sharing for fraud prevention. They also plan

to work with the FCA to understand transaction and data sharing opportunities, as well as looking to publish guidance by the end of 2025, starting with firm-level sharing but with an eye to bring industry-wide data sharing into scope. This is all welcome, but the review should carefully consider whether it is necessary to mandate data sharing on a statutory footing, and what this would take in terms of infrastructure and capabilities.

There is a limit, however, to what can be done purely by data sharing between PSPs, as much of the intelligence required to prevent fraud lies outside the sector, including with social media and telecommunications companies. This report will return to the question of cross-sector data sharing in Section 2.

Understanding consumer experience and awareness

One of the costs anticipated as part of the MRR was increased friction between consumers and PSPs. The PSR estimated a cost to consumers of increased friction and delayed payments of between £2 million to £30 million per year. The APPG also heard from PSPs that increased friction was an issue which led to some customers saying what they thought PSPs wanted to hear, rather than the whole story, in order to proceed with reimbursement. These dynamics emphasise the need to engage directly with both PSPs and consumers to gauge the impact of friction.

In addition, engaging directly with consumers can increase our understanding of awareness levels of the MRR, lending insight into what extent any potential drops in the volume of fraud recorded are due to prevention, and what is a function of low awareness and the MRR not being utilised to its full intention.

The independent review should include a consumer survey, in line with the FSCS Financial Lives survey, to fully understand how the MRR is impacting consumers in terms of their experience, attitudes and behaviour.

Mind the gaps – is the MRR is pushing fraud elsewhere?

As industry activity pivots to one type of activity, as do the tactics of fraudsters. Therefore, although the MRR may make it more challenging for fraudsters to scam over Faster Payments, that risks pushing their attention elsewhere, rather than deterring them altogether.

According to UK Finance data, across 2024 APP losses fell by two per cent to just over £450 million, but notably cases fell by 20 per cent – the lowest figure for both cases and losses since 2021. In the same period, however, unauthorised fraud jumped by 14% in terms of cases and 2% in terms of value.

The MRR is comprehensive when it comes to payments made via Faster Payments and CHAPS. This leaves gaps uncovered by the regulation which may become a target for fraudsters.

For example, there was a notable increase in APP fraud taking place between UK and international accounts, which lie out of scope of the MRR. International payments accounted for 11 per cent of APP losses in 2024, up from 6 per cent in 2023.

It is unclear at this early stage whether there is causation here or simply correlation. Either way, the independent one-year review must attempt to understand shifting patterns of fraud and the potential impact of the MRR on shifting fraud to other parts of the system, as well as how this should inform future action.

Evaluating the MRR – what the PSR has committed to

The PSR has committed to an extensive independent review process of the MRR. In PSR documentation, it commits to "regularly gather relevant data to monitor the effectiveness of the policy and to assess potential policy risks. This includes the potential risk of market exits, moral hazard, firms restricting customers' access to account and fraud migrating to other payment systems". Further information on the exact datapoints and issues they have committed to evaluate can be found here and here. The PSR has also confirmed that the review will look beyond the MRR to the wider policy programme to ensure a holistic assessment of APP fraud policy effectiveness.

The PSR issued the Invitation to Tender (ITT) for the independent review in early June, in which they set out a minimum scope of the work. As the work commences later this year, the PSR have confirmed that APPG report – and its suggestions on scope of the review – will be passed onto the independent party leading the evaluation, who can refine the scope if they feel it is appropriate.

The following recommendations are not, therefore, a comprehensive list of what the APPG believes the one-year review should evaluate. Instead, the recommendations emphasise areas of particular importance that should be examined 1) either to inform future changes to the MRR or other policies within the remit of the PSR and 2) to inform complementary measures that should be prioritised in the Fraud Strategy.

Recommendations – a broad and deep review

The APPG recommends that the independent one-year review and ongoing evaluation of the MRR, considers and undertakes the following measures:

Consumer focussed survey to understand the awareness of the MRR, its impact on increasing trust and confidence, as well as customer experience across the reporting and claims process.

Understand whether reports of fraud gone up, and if not, is that due to improved fraud prevention or a lack of awareness of the MRR?

Engage with the Financial Ombudsman Service to understand the experience of customers whose complaints are not resolved or disputed under the terms of the MRR, and to understand how many claims over £85,000 were successfully reimbursed after going to FOS.

Engage with PSPs to understand how they are implementing the MRR, especially in terms of how 'consumer standard of caution' is applied, as well as where cases have been deemed a 'civil dispute'.

Engage with PSPs to better understand the steps they have taken to improve detection and prevention, in order to assess whether further guidance, standards and support should be introduced in these areas, in collaboration with the Lending Standards Board.

Examine what difficulties smaller PSPs and non-signatories of the CRM have faced in preparing for and implementing the MRR.

Closely examine whether the MRR is inadvertently shifting fraud elsewhere, and if so where, including looking outside the PSR's remit to cryptocurrency.

Based off the review, the PSR should:

Closely examine whether further regulation is necessary to include International Bank Transfers, Credit Unions, Municipal Banks, or National Savings Banks that don't participate in the Faster Payment Scheme.

Assess whether the £85,000 reimbursement limit should be reviewed.

Additionally, the PSR should consider:

Whether to mandate data sharing on a statutory footing, and what this would take in terms of infrastructure and capabilities.

The MRR should be one part of a broader approach

Ultimately, with the problem of APP fraud already advanced and severe, the first priority has to be mitigating harm by protecting the victims of APP fraud. According to a PSR survey, the top priority of 67% fraud victims is getting their money back and that is the logical place to start.

Early signs are that the MRR is having its intended impact, and the APPG are encouraged that the PSR has committed to a comprehensive, independent review to understand the full impact, positive and negative, that the regulation is having.

Many of the biggest changes that need to happen when it comes to reimbursement, prevention and beyond lie outside the scope of the one-year review, and the mandate of the PSR.

The MRR – necessary, but not sufficient

Viewed in isolation, the MRR is necessary, but insufficient, and should only be viewed as a stop-gap solution. In the short-term, it blunts the financial impact for the consumer, but it does not remove the threat, with fraudsters still stealing from victims and potentially being pushed to other channels, both old and new. In addition, there are anticipated side-effects and risks of the MRR which cannot be controlled through tweaks to the regulation, nor through its success in achieving its stated aims. For example:

1. The MRR, even if it achieves intention, will place large costs on financial institutions.
2. The MRR, if effective, will likely encourage fraudsters into other kinds of fraud with weaker protections.

The goal of counter-fraud should be to stop it, and the MRR alone cannot achieve this. At the same time, now that the MRR is in force, it cannot feasibly be repealed, and nor should it. This forces us to apply a broader lens to tackling APP fraud, one which allows us to build on the successes and moderate the side-effects of the MRR.

> *The MRR cannot be an excuse for inaction, though, especially on the part of government. Instead, it should be the springboard for ambitious, wide-reaching action to fight APP fraud.*

Financial institutions cannot go it alone

Financial institutions have a crucial role to play in fighting fraud in the UK. For instance, their real time data and analytics, direct relationships with customers, and advanced prevention systems, are powerful tools in our collective arsenal. This is demonstrated by financial institutions effectiveness in tackling unauthorised fraud – banks prevented £710.9 million of unauthorised fraud through advanced security systems in the first half of 2024.

Financial institutions also stand to gain. More than 30% of victims choose to not continue with their financial institution following a successful fraud attempt. Trust is the foundation of all banking relationships – without it, customers are hesitant to deposit, borrow or invest.

Preventing fraud and protecting consumers builds trust

FSCS research asked consumers what concerned them most about financial services providers in the UK. At the top of this list, 53% of respondents said that 'Becoming a victim of fraud/scams' was their number one concern. The third biggest concern was 'A lack of protection for consumers if things go wrong'. In addition, when asked what would improve their trust in the financial services industry, improved consumer protection came out top with 54% of respondents.

A culture has developed in the UK where consumers can, rightly, expect financial institutions to protect them from fraud. The benefits of such a culture also bring risks – specifically the risk of myopia, viewing financial institutions as the beginning and end of fraud prevention and protection, and in so doing placing excessive burdens on financial institutions whilst also failing to comprehensively tackle the issue of APP fraud in all its multi-faceted complexity.

In the short-run, PSPs have been tasked with bearing a greater portion of the burden in protecting consumers from fraud. This will be unsustainable if the MRR is not seen as a stepping stone to a more balanced approach. There is a need for a holistic approach to tackling APP fraud. The Government's Fraud Strategy is a valuable opportunity to define this. In the long-run, PSPs will continue to play a crucial role but ultimately should only bear partial responsibility for addressing a problem for which they are only partially responsible.

The ultimate success of the MRR is contingent

The MRR and the UK's wider approach to counter-fraud are ultimately interdependent and contingent.

The only way some of the challenges, limitations and consequences of the MRR can be mitigated is through integration within a comprehensive strategy of complementary reforms, focussed both on reimbursement and beyond. It is what comes next which dictates the ultimate success and fairness of the MRR, and the broader fight against fraud.

The MRR is a key element of a holistic Fraud Strategy, and a holistic fraud strategy is key to the ultimate success and fairness of the MRR.

There can be no half measures in the fight against APP fraud, and this should only be the beginning.

Section 2

No half measures – a holistic approach to APP fraud

APP fraud is a multi-faceted problem which requires a multi-faceted solution, and the Government's announced update to the Fraud Strategy represents a crucial opportunity to prioritise a holistic approach – balancing approaches, responsibilities and liabilities – to tackle fraud in the UK and internationally.

As outlined earlier in the report, a holistic approach to APP fraud should comprise of following seven pillars:

1. **Ambitious**
2. **Collective**
3. **Collaborative**
4. **Comprehensive**
5. **Fair**
6. **Integrated**
7. **Agile**

Despite some encouraging steps, the UK's current approach falls short of these standards. This section of the report outlines measures that should be included within the updated Fraud Strategy which, taken together, amount to a blueprint for a holistic 'No half measures' approach to tackling APP fraud that succeeds across all seven pillars, and will position the UK as leading the global fight against frauds.

The strategy should prioritise a 'whole of ecosystem approach', including but not limited to:

1. Government
2. Regulators
3. Law enforcement
4. The criminal justice system
5. Technology companies
6. Financial industry
7. Cryptocurrency industry
8. The international community
9. The public

In a 'no half measures' approach to fraud prevention, the Government should use every tool within its arsenal to enable, incentivise and compel the whole ecosystem to play its part and collaborate.

Although no country has solved the problem of APP fraud, when designing a comprehensive strategy, we should also look to other countries on the frontline of battling APP fraud, who are experimenting with different approaches to the UK.

Closing the gaps in reimbursement

Addressing the cryptocurrency and international blind spots

While the MRR has strengthened protections for APP fraud over Faster Payments, it explicitly excludes transactions involving cryptocurrencies. Scams which take place over cryptocurrency platforms are characterised by the same social manipulation techniques as APP fraud, with romance, investment and impersonation scams all prevalent. As the MRR gains traction, it is likely that an increasing amount of fraud will be pushed onto crypto platforms.

Which? warns that under the current PSP-focussed regime, victims who fund APP fraud via cryptocurrency exchanges or wallets "fall through the cracks" of reimbursement protections. In fact, 20% of fraud victims surveyed by Which? reported sending money via a cryptocurrency website or app – yet these payments lie outside the Faster Payments scheme and so there is no guaranteed refund. This leaves a significant regulatory gap at a time when over £350 million has estimated to have been lost to crypto fraud in 2024 alone. Currently, the crypto industry is largely unregulated, and although the FCA has made clear its intention to regulate, in the meantime gaps remain.

Absent an equivalent framework to the MRR, the crypto industry does not have the same cost-allocation incentives that drive bank to investment in fraud prevention, issue robust customer warnings, integrate pre-transfer screening, or drive customer education.

We do not have an accurate perspective on the scale of authorised fraud that takes place over crypto. The best data we have is from the PSR and UK Finance, both of which exclude crypto, and yet Refundee, an investigative company that helps victims recover funds, reports that Crypto scams now account for 37% of their roughly 5,000 annual cases. Fraud prevention should be a core part of the government's future regulation strategy for crypto, including gather data on the volume and value of fraud taking place across their platforms.

It is too early to assess the ultimate impacts of mandatory reimbursement, but pending the verdict of the independent one-year review of the MRR, the government should consider incorporating fiat-to-crypto rails into reimbursement rules and establishing a parallel reimbursement regime, which would not only protect victims but also incentivise crypto firms to collaborate in real-time data-sharing frameworks alongside financial institutions, technology companies, and law enforcement.

International payments

Another gap in reimbursement is international payments. Data reveals a notable increase in fraudsters tricking people into sending money abroad. International payments accounted for 11% of APP fraud losses in 2024 – almost double the 2023 figure. While PSPs themselves are seeing an increase, remittance platforms and payments platforms specialising in international transfers are especially vulnerable to this increase.

Once again, pending the findings of the independent one-year review of the MRR, the upcoming Fraud Strategy should consider introducing a mandatory reimbursement requirement for international transfers and remittance services, obliging firms to reimburse victims of APP fraud on cross-border transaction, enforced by the FCA.

These measures are essential in ensuring that the Government's approach to fighting fraud is integrated and collective, rather than siloed. It would also incentivise greater cross-sector collaboration. There also cannot be one standard for some and different standards for others. Mandatory reimbursement for crypto platforms would also increase fairness, ensuring financial institutions are not held to a different standard to other platforms where fraud takes place.

As the PSR is absorbed into the FCA, which is set to have its remit expanded to further regulate the crypto industry, there should be greater opportunities to streamline regulation between payment systems. The FCA has recently concluded a consultation on the regulation of specific cryptoasset activities as part of its 'Crypto Roadmap'. We recommend that the following recommendations are integrated within the Fraud Strategy and the FCA's roadmap.

Recommendations

- **Consider expanding the MRR to cover fiat-to-crypto transfers over UK payment systems,** (pending the judgements of the independent one-year review of the MRR) so that both sending PSPs and crypto deposit receivers share liability under the 50:50 cost-share model.
- **Fraud prevention should be a core part of the government's future regulation strategy for crypto,** including gathering data on the volume and value of fraud taking place across their platforms, and improving customer education on their platforms.
- **Consider introducing a mandatory reimbursement requirement for international transfers and remittance services,** (pending the judgements of the independent one-year review of the MRR), obliging PSPs to reimburse victims of APP fraud on cross-border transactions, enforced by the FCA.

Maintain and enhance the Financial Ombudsman's powers in absence of greater regulation

The above speaks to the regulatory gaps in protection that consumers currently face. Although progress is being made, it is likely that it will take time to bring in regulatory protections. In the interim, the Financial Ombudsman Service (FOS) provides an essential last line of consumer defence through its 'fair and reasonable' remit.

In fraud cases, the 'fair and reasonable' remit allows the FOS to consider whether a bank should have taken an action that is not specifically described in regulation but is considered good industry practice. Many APP fraud cases that reach the FOS relate to payments that are not covered by the MRR (or previously the CRM). Most commonly, this is because payments are made internationally or to a cryptocurrency exchange.

Case study – Mr G

In 2021, a 75-year-old-man had recently lost his wife and was isolated during COVID lockdowns. After clicking on a Facebook advert for investment advice supposedly endorsed by Martin Lewis, he was contacted by a representative of the scam firm and was tricked into investments totalling £130,000. The money was sent through international payments and cryptocurrency, neither of which are covered by the MRR.

The bank was aware that MR G had never made large payments internationally or to cryptocurrency, and that these payment methods are commonly targeted by fraudsters. Despite serious red flags the bank did not phone the customer to understand what was happening. The bank stated that the payments were not covered by regulation and, therefore, they would not be reimbursing Mr G for his loss.

After an investigation by the FOS, they determined that there was a clear change of behaviour on Mr G's account, which is commonly associated with APP fraud. APP fraud is not new, and therefore it was fair and reasonable to expect the bank to have identified that the transactions were unusual. They determined that if the bank had taken action, it would have likely been able to prevent the fraud losses.

Source – Refundee

In a recent Policy Paper from HM Treasury, questions were raised about whether the FOS should be stripped of its power to decide what is 'fair and reasonable' in individual cases.

It is an imperfect system, as there should be rules in regulation in place to provide clear guidance and precedent, but as fraud trends move faster than regulation, the FOS should maintain its powers as an essential backstop for consumers. Stripping this discretion would leave victims without a backstop and remove a key incentive for firms to adopt robust fraud-prevention and customer-care practices.

The Fraud strategy should also focus on how to provide similar backstop protections for crypto activities, which currently do not fall under the FOS's remit (except a PSP's handling of a Faster Payments deposit into a crypto-exchange's account – because accepting and transferring fiat money is a regulated payment service). This could potentially be in the form of a temporary extension of the FOS regime to cover crypto asset activity itself, although this could be challenging given the existing resource constraints faced by the FOS. On this point, the Fraud Strategy should commit to increasing the funding of the FOS, so it is better equipped to handle the quantity of cases it receives.

For more complex or high-value disputes – especially those involving SMEs or novel payment types – the FOS's informal, case-by-case approach can be inadequate. Legal commentators, along with the APPG on Fair Banking have long argued for a permanent, specialist Financial

Services Tribunal to provide a fast, inexpensive tribunal model akin to Employment Tribunals. Such a tribunal would offer clearer precedent, binding interpretations of law and regulation, and an appeals mechanism.

This would have broad benefits in terms of addressing complex fraud cases, increasing certainty, and beyond. Transitioning to this model would preserve the FOS's accessibility for everyday cases while ensuring that higher-stakes or novel disputes receive the specialist adjudication they deserve. In the meantime, complex fraud cases should remain with FOS, rather than being shifted outside to the police or the FCA.

Recommendations

- **Commit to maintain the FOS' 'fair and reasonable' remit** to ensure consumers harmed by novel or unregulated fraud – such as those involving cryptocurrency or cross-border transfers – have access to redress when rigid rules fall short.
- **Commit to increasing funding of the FOS**, so that it is better equipped to handle the quantity of cases it receives.
- **Legislate to create a specialist Financial Services Tribunal,** empowering it to deliver swift, expert adjudication and binding precedent for complex and high-value financial disputes beyond the scope of the FOS. In the meantime, complex cases should remain within FOS remit.

Renewed attention on fraud towards business

While the 2023 Fraud Strategy acknowledged that "Predatory criminals take money out of the pockets of hard-working people, businesses, and organisations", in practice it placed much stronger emphasis on protecting consumers."

This is also reflected in the MRR. In the first half of 2024, business losses comprised £47.2 million out of a total of £213.7 million. Under the MRR, only micro-enterprises with fewer than 10 employees and a turnover of £1 million are eligible for reimbursement. This protection is valuable but leaves many SMEs out of scope. This speaks to a wider under-consideration of the risks fraud poses to business.

This consumer centric focus is problematic: businesses – particularly SMEs – face growing exposure to cyber fraud and APP fraud yet lack the same layer of tailored support or mandatory protections. Ignoring business-specific fraud vulnerabilities leaves a significant gap.

Recommendations

- **The Fraud Strategy should ensure that it is has a renewed focus on understanding the impact of fraud on businesses,** and what can be done to better protect businesses from fraud and support them in prevention efforts.

Prevention at the strategic heart of counter-fraud

Reimbursement is only necessary as APP fraud continues to occur. Fraud prevention is ultimately the best form of consumer protection, and the best way to reduce the burden of reimbursement sustainably. A comprehensive approach must therefore have prevention at its core and that can only happen effectively by harnessing the capabilities and resources of the private sector.

Prevention cannot happen without social media

The elephant in the room when it comes to preventing fraud has long been the enabling role of social media and telecommunications. The latest UK Finance data shows that 70 per cent of fraud cases are enabled by online sources, accounting for 29 per cent of total losses. Over half of scams involve Meta platforms: in 2023, Meta platforms (Facebook, Instagram, WhatsApp) were linked to 54% of scam incidents (119,338 cases) and 18% of total losses (£62.7 million). That's roughly £1 in every £5 lost in scams. 16 per cent of cases are enabled by telecommunications, which are usually higher value cases accounting for 36 per cent of losses.

> *"If Meta was a building in the middle of a town centre, and criminals were acting through that building, then it would be very quickly shut down. As it is, these platforms are remote, so there's a level of disassociation, whereby people accept fraud as part of their everyday life. We need to change this mindset and really present this as the serious issue it is."* – APPG roundtable participant

The previous Fraud Strategy relied heavily on voluntary charters (e.g. the Online Fraud Charter) which have not materially reduced scam losses. Which? research found that 6.6 million consumers lost money to online scams in the year since the signing of the Charter. When asked whether they trusted online platforms more than when the Charter was introduced, 34% of respondents said they were less likely to trust them. Only 3% felt more confident.

The challenge is that the nature of social media and their role in enabling fraud makes it challenging to adequately incentivise them, in large part due to the scale of leading platforms. The sheer quantity of users and inelasticity of demand means instances of fraud, although harming trust, do not materially damage the largest platforms. Financially incentivising some of the largest companies in the world is also a challenge. In 2024, Meta's revenue was $164.5 billion, dwarfing the scale of fraud that originates on their platforms.

The new Fraud Strategy must be more ambitious in order to incentivise participation and collaboration in a collective fraud response. There are several tools the Government has at its disposal.

Introduce a tech levy

The Government could extend the Economic Crime Levy to tech, social media and telecoms firms, which UK finance estimated could "raise over £40 million a year". In the short-term, this would provide valuable resources for law enforcement to "invest in better technology and recruit specialist officers and incentivise action to reduce fraud."

A flat fee risks being inconsequential for Big Tech as an incentivising force, so the Government should consider a sliding scale or performance-linked surcharge, such as an additional levy for failure to meet fraud-takedown KPIs, which could make the financial impact more material.

Explore liability sharing for fraud reimbursement

There is a growing chorus, especially among the financial industry, for social media to become liable for sharing the cost of APP fraud reimbursement. This comes with extensive practical challenges, as there is a difference between the execution of fraud and the enabling of fraud and therefore establishing a fair cost share is difficult. The Fraud Strategy the Government should commit to scoping the possibility for shared reimbursement. This is essential in determining a fair and collaborative approach to APP fraud.

Who should pay for reimbursement?

When asked by the Global Anti-Scam Alliance, 'if you were scammed, who do you think should be responsible for making sure you are paid back for your loss, almost 50% said that 'my bank, payment method or crypto exchange I used' should be responsible. Roughly 25% of respondents said the 'Online platform used by the fraudster' and 25% said the 'Website provider / host used by the fraudster' should pay.

Put the Online Fraud Charter on statutory footing

The Online Fraud Charter led to some welcome steps and further demonstrated the benefit the technology sector's involvement. To prevent gaps and ensure a response to comprehensive, the actions included in the Online Fraud Charter should form the basis for statutory legislation. This would include mandating enhanced Know your Customer (KYC) requirements (potentially utilising new forms of digital ID), and requiring social media companies to participate in cross-sector data and intelligence sharing initiatives.

Bring forward implementation of the Online Safety Act and strengthen Code of Conduct

The Online Safety Act, which passed into law 2023, has great potential to hold technology firms accountable. The current timetable, however, means that certain duties, including those regarding fraudulent advertising, may not be in effect until 2027. The strategy should commit to bringing forward implementation of the Online Safety Act. In addition, the measured in the Code of Conduct for fraudulent content under the Online Safety Act could be significantly strengthened.

Together, these actions would ensure that technology and telecoms companies play their part in a collective, collaborative fraud response.

Looking to Australia

Under Australia's Scam Prevention Framework, social media companies are regulated entities bound by six core principles, including proactive monitoring and rapid scam-content removal. Social media platforms must verify all financial-product advertisers, ensuring only authorised entities can place payment-related ads. They are also required to swiftly suspend or remove user accounts, advertisements or messaging channels flagged for scam activity, with civil penalties of up to AUD 50 million for serious or repeated breaches. Moreover, regulated social-media firms must report actionable scam intelligence to the National Anti-Scam Centre via Scamwatch, fostering real-time data sharing with law enforcement to counter evolving fraud tactics.

Recommendations:

- **Introduce a tech levy** to raise vital funds for the counter-fraud response.
- **Scope possibility for reimbursement cost-sharing** between financial institutions and those responsible for enabling fraud.
- **Mandate action by social media firms** by placing the Online Fraud Charter on statutory footing.
- **Bring forward the implementation of the Online Safety Act,** and strengthen Code of Conduct for fraudulent content.

Enabling prevention through data sharing

Tackling fraud is much like solving a jigsaw puzzle: without all the pieces, it is impossible to fully understand or prevent APP fraud. Data and intelligence sharing is at the heart of this, and the Government has a crucial role to play in enabling it.

The need for a unified approach to data sharing

It is widely acknowledged by those within the anti-fraud space that data sharing is a necessity for effectively fighting fraud. And yet, at present, the existing system of data sharing is highly fragmented, with clear inconsistencies. While significant data collection efforts are made by several individual players – Cifas, UK Finance and Pay.UK to name a few – the lack of connection between them poses a real problem.

The idea of data sharing is not a new concept. As outlined in their report, following an investigation in 2022, the House of Lords Fraud Act 2006 and Digital Fraud Committee highlighted that "Information sharing is a critical component to the counter-fraud effort and must proactively be encouraged by regulators and legislation." Yet, since this comment was made, very little progress has been enacted in the way of either regulatory or legislative action to encourage data sharing.

Why share data?

While there are many justifications for data sharing to address APP fraud, three principal motives are:

1. **Preventing fraud:** A holistic, cross-sector view closes the gaps that fraudsters often exploit between institutions, whilst real-time sharing of suspicious indicators – such as scam URLs or unusual transaction patterns – acts as an early-warning mechanism, allowing potential fraud to be flagged and disrupted before significant losses occur.
2. **Establishing patterns of fraud:** Data sharing is an essential component of an integrated approach to fraud prevention, enabling a comprehensive understanding across fraud types, track shifting patterns of fraud, and supporting agile, adaptive responses.
3. **Lessening the burden on PSPs:** Enhanced cross-sector data sharing would improve visibility into fraud origination points, enabling platforms to spot fraud earlier and prevent it from taking place, ultimately reducing reimbursement costs.

While initiatives like Meta's Fraud Intelligence Reciprocal Exchange (FIRE) – allowing for banks to share transaction intelligence with the platform – are important first steps, the argument always loops back to the need for a coordinated, cross-sector response. The overwhelming call is for a 'unified data sharing response', that tackles APP fraud with 'whole-of-ecosystem' collaboration.

To move beyond the siloed and piecemeal data sharing efforts, it is necessary for the Government to actively enable a unified data sharing response.

Government action is key to enabling effective data sharing

> *"Within proper legal and procedural guardrails, arming the private sector with the data and intelligence they need to scale disruptive prevention is, arguably, their [the Government's] only option."* – Helena Wood, in RUSI

The necessary frameworks and assurances to enable effective and lawful information exchange remain underdeveloped. It is therefore imperative that the Government takes a leading role in removing these barriers and providing the clarity, infrastructure, and legislative support required for scalable, coordinated data sharing.

One of the most pressing challenges is the lack of robust infrastructure to support cross-sector data sharing. The establishment of a centralised data-sharing platform would offer a critical step forward. Such a platform would serve as a hub to consolidate existing efforts, facilitate real-time information exchange, and standardise processes across financial institutions, telecoms, online platforms, law enforcement and Government agencies. This could sit within the pre-existing National Economic Crime Centre, establishing it as the driver of intelligence development and data analytics. This would enable more agile public–private data and enable a more coherent intelligence-led approach to prevention.

Overcoming ambiguity

While the ICO has made it clear that data protection is not an excuse when tackling scams and fraud, many organisations – particularly outside the financial sector – remain hesitant to share personal data due to perceived risks around breaching GDPR. The Information Commissioner's Office (ICO) has issued guidance confirming that such data sharing is permissible within the UK's data protection framework, provided it is conducted responsibly, proportionately, and with appropriate safeguards.

However, ambiguity persists around how organisations should apply these principles in practice. To address this, the Government must go further in issuing detailed, practical guidance, aligned with the ICO's position, on how firms can confidently share data in compliance with GDPR. The forthcoming Data Use and Access Bill, which proposes introducing 'recognised legitimate interests' as a legal basis for crime prevention, is a welcome step. Still, to be effective, it must be accompanied by implementation guidance that ensures legal certainty and operational clarity for all participating sectors.

As well as informing the Fraud Strategy, the following recommendations should feed into the upcoming Economic Crime Data Strategy[1].

Recommendations

- **Enable data sharing through a centralised platform** to coordinate cross-sector intelligence, standardise practices, and enable real-time collaboration across the fraud prevention ecosystem.
- **Provide clear, practical guidance on how data sharing is GDPR compliant** to ensure legal certainty and compliance.

Providing an effective deterrent to fraud

Although the private sector is crucial to preventing fraud, the fact that fraud is ultimately viewed as a "low risk, high reward" reward crime is due to inadequate enforcement. Roughly 60% of Britons surveyed say that the UK's ability to arrest fraudsters is either bad or very bad, a perception which impacts whether or not victims of fraud report it. Reforms are needed across the counter-fraud response, from reporting, investigation, arrests, and prosecutions.

Reforming fraud policing

Ensuring stable core funding

Fraud accounts for 40 percent of reported crime, yet only 2 percent of police funding is dedicated to it, illustrating a stark mismatch in resource allocation.

Fraud was classified in 2023 as a National Security Threat, giving it the same status as terrorism. It should be treated as such. Other areas of national security policing receive ring-fenced funding, whilst funding of policing is "piecemeal, fragmented and allocated on an unsustainable basis", argue Cifas in their counter-fraud pledges.

There is a need for stable core funding, and the Government should commit to providing ring-fenced, multi-year funding for fraud policing. Stable funding of this kind provides long-term certainty to policing, which in turn attracts staff to move to fraud policing who may previously have been deterred by unstable fund-based budgets.

Establish an Economic Crime Fighting Fund

On top of reinforced core funding, the establishment of an Economic Crime Fighting Fund would provide a cost-neutral addition to policing budget. The fund would reinvest a portion of fines and seized criminal assets directly back into policing budgets, creating a self-sustaining, ring-fenced financing mechanism that avoids additional taxpayer burden. Spotlight on Corruption finds that if 50% of the sums generated for Government from economic crime enforcement were reinvested, economic crime regulation and enforcement would have stood to gain £233 million a year, nearly double the annual investment underpinning the 2023-2026 Economic Crime Plan. In combination with a tech levy, this would transform law enforcement's capacity to deter fraud.

Sustainable, ring-fenced, multi-year funding, topped up with innovative financing mechanisms, is essential in providing a meaningful fraud deterrent.

Streamlining policing

The Fraud Strategy should stabilise the policing landscape after decades of uncertainty and debate around respective roles within the system. A single command structure with clear powers is needed to coordinate activity.

The City of London Police should function as this single command structure, acting as the policing lead for economic crime, with ringfenced assets at the regional tier of policing. The CoLP would also have responsibility for setting a national policing strategy for economic crime across the wider 43-force structure.

The single command structure should oversee regional fraud teams, which have seen a much welcomed recent expansion. These regional fraud teams, which would remain within policing, should be expanded, and in the future could be developed into regional economic crime 'super-hubs' which bring together a range of enforcement, regulatory and private actors, proactively investigating and driving large-scale disruption and prevention.

Together, this would create a clear, streamlined and agile policing response.

Targeted disruption rather than mass prosecution

A RUSI paper on economic crime policing argued, "the government's strategy remains fixated on outdated metrics of arrests and prosecutions". A high-volume crime which often originates overseas (explored in the following section) requires a different approach to traditional justice outcomes.

In conversations held between the APPG and stakeholders, it was emphasised that systemic issues, such as a lack of space in prisons, also warn against relying solely on the volume of prosecutions as a deterrent. Quality action must take precedence over quantity. As Helena Wood writes, police action should:

"be reserved for more targeted and 'surgical' operations against the enablers of mass-scale fraud; the criminal marketplaces offering 'fraud as a service' capabilities to organised fraud groups."

The Government should focus on more targeted operations therefore, focussing on 'online and upstream' interventions.

Case study – Operation Elaborate

Operation Elaborate, led by the Metropolitan Police's Cyber Crime Unit, proactively targeted iSpoof.cc – a spoofing service that enabled criminals to disguise their caller ID and defraud victims. Between June 2021 and July 2022, iSpoof facilitated around 10 million spoofed calls globally (3.5 million in the UK), resulting in estimated losses exceeding £50 million. The multi-agency crackdown involved the Met, City of London Police, Netherlands Police, Europol and Eurojust, culminating in the site's takedown and over 100 arrests as suspects behind the fraud network were identified and detained.

Recommendations

- **Commit to providing stable core funding for fraud policing,** which is ring-fenced and multi-year, in line with policing for other national security threats.
- **Establish an Economic Crime Fighting Fund** to support funding for fraud policing.
- **The City of London Police should function as a single command structure,** acting as the policing lead for economic crime, setting a national policing strategy, with ringfenced assets at the regional tier of policing.
- **Fund a stronger network of Regional Economic Crime Hubs** to proactively investigate complex cyber-enabled fraud, with the aim to develop Regional Economic Crime Super Hubs in the future.
- **Policing should prioritise a 'quality' over 'quantity' approach,** focussing on more targeted police operations and 'online and upstream' interventions.

Criminal justice fit for a 21st century crime

Fraud prosecutions plummeted by 64.6% between 2017/2018 and 2022/2023, in part because of the inadequacies of the criminal justice system in prosecuting a 21st century crime.

Dedicated Courts

On top of low referrals from the police, fraud trials are often subject to considerable delays, particularly with the growing backlog of Crown Court cases, where the majority of fraud trials have historically been dealt with. Fraud cases are often down deprioritised compared to those involving physical harms or where offenders are in custody. Delays also occur due to the complexity and size of some fraud cases. Delays of cases that do go to court may last for several years, meaning victims are left in limbo, and fraudsters may continue to offend while waiting for the case to be heard in court.

Dedicated courts which focus on economic crime and fraud are necessary to counter this. According to Cifas the planned Central London Economic Crime Court is a blueprint for a modern criminal justice response to fraud, cyber and wider economic crime. Once delivered, it should be considered how this model can expand and scale across regions.

Ensure sentencing reflects the societal harms of fraud

The current sentencing guidelines for fraud have two key issues:

1. **Outdated maximum sentences:** The Fraud Act 2006 caps custodial sentences at ten years, focussing primarily on financial loss and ignoring the profound emotional, psychological and societal harms modern APP fraud inflicts.
2. **Insufficient victim-centred sentencing**: Unlike guidelines for crimes such as assault – which explicitly factor in psychological distress – the fraud framework remains narrowly tied to monetary thresholds, undermining deterrence and failing victims.

Recommendations

- **Consider how the model of the dedicated Central London Economic Crime Court can be expanded across regions**.
- **Revise sentencing guidelines** to reflect the societal harms of fraud.

A global response to a global problem

The issue of APP fraud is beyond the scope of UK law enforcement to handle alone. It is estimated that 70% of fraud now includes an international element. Much of this takes place within organised gangs, who are increasingly targeting fraud as a 'low-risk, high-reward' alternative to higher-risk activities more commonly associated with organised crime, such as narcotics or trafficking. Scams are big business, with research by the US Institute of Peace estimating that these scams generate $63.9bn a year in global revenue.

Recent journalistic work has put the international dimension of fraud under the spotlight. The Economist's podcast series 'Scam Inc' visited notorious 'scam farms' in Myanmar, where individuals are trafficked and held, forced to carry out online scams for organised gangs. Similarly, a recent investigation from the OCCRP exposed the inner workings of two scam call centres in Israel, Eastern Europe, and the country of Georgia, whose employees have convinced at least 32,000 people to make investments worth at least $275 million[2].

In announcing the strategy, Lord Hanson emphasised that "global co-operation will be key to tackling this growing issue." The benefits of collaboration go beyond the UK, as work to crack down on scams stands to benefits individuals around the world who are victims of fraud.

Collaboration on targeted enforcement and intelligence sharing

Much of the intelligence necessary to prevent and disrupt fraud lies beyond the UK's borders. The strategy should demonstrate commitment to collaborating with international law enforcement agencies on coordinated efforts, along with financial intelligence units and regulatory agencies to determine how best to tackle fraud internationally.

This may require bilateral partnerships and MOUs between countries to formally detail cooperation on financial intelligence, enforcement, and evidence sharing.

The UK should also establish technical assistance programmes with priority fraud 'source' countries who themselves lack the resources to fight fraud, via its development assistance programme. This must be coordinated with the FCDO and integrated into their priorities.

Much like local enforcement, collaboration should target quality intervention over quantity, hitting the arteries of organised fraud.

Case study – Genesis Market

Genesis Market was a platform which hosted around 80 million stolen credentials and digital fingerprints worldwide. In 2023, it was taken down by a coordinated operation which seized the marketplace's servers and infrastructure. Led by the FBI, Dutch National Police and the UK's National Crime Agency, and involving 17 countries, the operation led to 24 arrests in the UK and 120 arrests and over 200 searches globally.

The role of China – counter-fraud as diplomatic priority

There are international hotspots which will require careful targeting. The UN says that in 2023 the industry employed just under 250,000 people in Cambodia and Myanmar alone, with another estimate putting the number of workers worldwide at 1.5m. Of the $63.9bn a year in global revenue, $36.9 is estimated to be generated in Cambodia, Myanmar and Laos. In these places, fraud has become a mainstay of the economy, and collaborating directly will be challenging. It is necessary to look to third parties.

China, given its influence in the region, must play a key part in tackling organised fraud. According to the Economist, many scam bosses are from mainland China, with the Chinese Communist Party arresting hundreds of thousands of alleged fraudsters each year. China has demonstrated its effectiveness in tackling scams when they affect its citizens. Now careful diplomacy is required to ensure they are a key part of a globally co-ordinated counter-fraud response.

Co-operating with China on counter-fraud should be a diplomatic priority of the UK, necessitating further collaboration between the Home Office and Foreign Office in tackling fraud.

Case study – the disappearance of Wang Zing

In January 2025 Chinese actor Wang Xing went missing. He had been deceived into a scam centre in Myanmar by a fraud group under the pretext of "going to Thailand for filming". On 7 January, a joint Chinese–Thai law-enforcement operation located and rescued him from a scam centre in Myanmar. The publicity of this case triggered wider action from Thai authorities, who cut the supply of electricity, internet services and fuel to five areas in Myanmar. By February 13th, it was reported that up to 8,000 workers in the scam parks, mostly Chinese, were to be evacuated, spurred by increase Chinese collaboration with local authorities and international outrage.

Showing global leadership

In 2024, the UK Government showed significant leadership by hosting world leaders for the first Global Fraud Summit. This should be the starting point for the UK to be a global leader on counter-fraud.

It should do this by driving forward the development of international architecture to enable global cooperation on fraud prevention and sharing of best practice. The UK can lead on building a 'coalition of the willing' with key partners to drive a new global approach. In addition, international collaboration requires structures and framework. For example, anti-

money laundering has the Financial Action Task Force (FATF), an international organisation with a mandate to combat money laundering. No such organisation exists for fraud, and the UK should lead on the establishment of such a body.

Recommendations

- **Formalise international partnerships,** including negotiating bilateral MOUs with foreign law-enforcement agencies, financial intelligence units, and regulators to enable secure, real-time data, evidence and intelligence sharing.
- **Deploy technical assistance to 'source' countries** to build capacity in high-risk jurisdictions.
- **Focus on high-impact interventions,** targeting the "arteries" of organised fraud through joint task forces and precision enforcement – rather than broad, low-yield cooperation – to disrupt the most harmful networks.
- **Elevate China as a strategic partner,** making diplomatic engagement with China a priority, leveraging its regional influence and recent domestic anti-scam actions to tackle cross-border scam operations.
- **Champion a global coalition,** building on the Global Fraud Summit by spearheading an international architecture or "coalition of the willing" to drive a unified, UK-led approach to fraud prevention and victim protection.
- **Lead on establishing international fraud architecture,** by working to establish an equivalent body to FATF that oversees and coordinates international counter-fraud efforts.

The UK as a fraud enabler

Fraud is not simply something that happens to the UK, it is enabled by it. Fraud is a predicate offense, meaning it is a criminal activity that generates illegal proceeds which are then laundered. The problem is diverse, whether it be through opaque corporate structures in the UK and in our overseas territories, or via the UK's network of professional enablers.

By enabling money laundering, the UK shoots itself in the foot on fraud.

The strategy should explicitly recognise the UK's role in enabling illicit financial flows, including the laundering of the proceeds of fraud, and commit to pursuing reforms which ensure the UK is not a haven for dirty money[3].

Money-laundering goes beyond fraud, necessitating that the Fraud Strategy is properly integrated within the Government's broader Economic Crime Plan (ECP), where fighting illicit finance is a priority. It is essential that the fraud strategy explicitly recognises and acknowledges the interconnections across the ECP, how it plans to collaborate cross-department where there are dependencies, ensuring that workstreams don't become siloed.

Recommendations

- **The strategy should recognise that solving fraud requires a focus on the onward laundering of fraud proceeds,** and ensure it focusses on the problem of fraud from end to end, recognising the role the government has to play at each stage.
- **Ensure the strategy is adequately integrated into the broader Economic Crime agenda** and working cross-department to end the UK's role as an enabler of fraud.

Building a fraud resilient population

Consumers are not only the primary targets of fraud but also essential to its prevention. The development of a fraud-resilient population – capable of identifying and responding to fraud risks – is an area in which Government leadership is crucial. With the tools and infrastructure at its disposal, the UK Government is well positioned to take an active role in empowering consumers through targeted education and awareness initiatives.

Education from all angles

IDNow's 2024 report found that nearly half of survey respondents were unaware of deepfakes, and one-third admitted to sharing ID documents via insecure channels. Furthermore, a separate study notes the significant demographic disparities in fraud awareness, with 27.9% of those aged 25-34 rank APP fraud as a primary financial threat, only 8.4% of those aged 65+ see it in the same regard.

Moreover, as the UK moves toward a 100% reimbursement model, there are concerns consumers will become complacent and less diligent when it comes to spotting fraud. In this regard, consumer education is necessary in ensuring that the risk of APP fraud remains at the forefront of people's minds, despite increased reimbursement.

Consumer education also plays a critical role in destigmatising fraud and normalising the experience of fraud. Effective education not only helps to alleviate the emotional burden associated with fraud but can also increase the likelihood that victims will report such incidents, thereby enhancing overall prevention and response efforts.

What is already being done?

The foundation for consumer awareness is in place, with several non-governmental initiatives leading the way.

Case Study – Take 5 To Stop Fraud

UK Finance's "Take Five to Stop Fraud" campaign is chief among existing educational initiatives. The campaign follows a simple but powerful message: Stop (pause before sending money or personal information), Challenge (question any requests that seem suspicious), and Protect (report any suspected APP fraud scam immediately to Action Fraud). Its provision of both educational resources and business-centred advice act as powerful tools to educate consumers about risks and ways to protect themselves against APP fraud.

Case Study – Scam Interceptors

Co-produced by the BBC and the Open University, Scam Interceptors is a TV programme that shows ethical hackers infiltrating fraudsters' systems to disrupt live instances of fraud, aiming to prevent the financial losses caused by fraud. Televising the action taken by those on Scam Interceptors serves an important educational tool, demonstrating to the public what a scam can look like and what to do if they think they are being scammed.

Alongside these examples, financial institutions and PSPs have also taken their own initiatives to educate their customers. Examples include Metro Bank's 'Be Your Own Hero' fraud awareness campaign, and Barclays' 'Little Book of Big Scams'. Many banks and PSPs also use scam alerts, both through online banking platforms and other services like ATMs, to alert customers to the risk of APP fraud.

The Government should coordinate an 'Educate from all angles' approach

As the FCA has noted, putting consumers first involves not only protecting them from harm but also equipping them with the knowledge to identify and respond to fraud. It is ultimately the Government who must lead the charge in fostering an informed, aware and equipped population. It should do this via an 'educate from all angles' approach.

Case Study – Public scam awareness in Singapore

The Singaporean Government has invested heavily into public awareness campaigns – such as the immersive 'Unpacked' experience and the Scam Public Education Office's TikTok 'Scam-tastic' challenge. Singapore's approach is widely recognised for its innovation and impact, with platforms like TikTok citing it as a leading example of how governments can harness social media and community engagement to build digital resilience and reduce scam vulnerability.

The strategy must commit to increasing awareness as to the resources and tools available to them. For instance, reporting instances of fraud is crucial for understanding the scale of fraud and addressing it, and yet the National Crime Agency estimates that 86% of frauds go unreported. A recent survey showed that over 30% of respondents were unsure where to report scams, and almost 20% said it was too complicated. With the Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) will replace Action Fraud this year and it is essential that the public is aware of the service and how to use it effectively.

In addition to direct leadership, the Government should seek to mobilise a broader range of stakeholders capable of fulfilling an educational role. To ensure broad and equitable reach, consumer education must span forum – including schools, workplaces, public institutions, and community settings – and utilise both digital and non-digital mediums such as online platforms, broadcast media, print materials, and physical advertising.

A good example of this 'all angles' approach is Cifas, working with the PSHE Association have called for financial harms education to be mandatory at KS3 within the PSHE education syllabus.

Finally, to ensure long-term effectiveness, consumer education efforts must be future proof. Fraud patterns shift, and tactics and technologies evolve. An 'educate from all angles' approach must prepare consumers for a dynamic threat landscape. By equipping the public with knowledge across fraud types, Government can help foster an agile, fraud-resilient population capable of adapting to evolving criminal behaviour.

Improving victim support

As it stands, the system is failing the victims of fraud. Some vital measures have been taken – reimbursement is crucial for victim support, for example, but does not address the root of the issue. Many of the suggestions outlined in this report will also boost victim support. Reassuring victims that something will be done, or at least providing insight to the process, is essential support, but currently only 1 per cent of reports received by Action Fraud annually lead to criminal charges or prosecution. Enhanced support to law enforcement supports this, but it is also crucial that the new Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) actively prioritises victim support.

The effects of fraud can be psychologically devastating. According to Nik Adams, assistant commissioner at the City of London police, 300 people a year are referred to their local force after reporting a scam due to suicide risk. Invaluable tools exist, such as Victim Support. Awareness of pre-existing tools should be increased, including through the new FCCRAS. Additionally, more regional in-person support should be provided to the victims of fraud.

The Fraud Strategy should actively commit to supporting victims so that they are not defrauded again. One of the biggest indicators of vulnerability to fraud is having been defrauded before. In the financial year 2019/2020, over £373 million was lost by repeat victims of fraud, with the average loss reported by repeat victims 14 times higher than the average victim. The strategy should commit to providing tailored training, resources and support to ensure victims are not defrauded again.

Supporting the vulnerable in the face of a 21st century crime

Fraudsters target vulnerabilities. No one is immune from fraud, but the risk increases if individuals have certain characteristics of vulnerability.

According to the 2022 FCA Financial Lives Survey, vulnerability can be split into 4 drivers: poor health, negative life events, low resilience, and low capability. In 2022, 47% of UK adults exhibited one or more characteristics of vulnerability.

Vulnerability increases fraud risk

Among adults with no vulnerability characteristics, 68% say they always or sometimes:

- *Cover their PIN when using an ATM or paying with a bank or credit card*
- *Securely dispose of any statements or documents containing financial information*
- *Verify that a website is secure before entering bank or card details*
- *Check their statements for unfamiliar transactions*

By comparison, just 54% of adults in vulnerable circumstances follow these practices, and the figure falls to 42% among those with low financial capability.

Those with low financial capability are particularly vulnerable to fraud. This is something that can be directly supported. For example, the proportion of adults with characteristics of vulnerability actually fell from 51% in 2017 to 47% in 2022, driven primarily by a reduction in the number of old people who were digitally excluded (a low capability characteristic). The strategy should endeavour to support those with low financial capabilities through education and training schemes.

At the same time, there are vulnerabilities which primarily lie outside of the remit of the fraud strategy, such as 'low financial resilience' which has increased, as has 'poor health', including mental health.

Fraud has been described as a 21st century crime, and it is, but not only in terms of the technology it leverages.

Fraud preys on the vulnerabilities of our time – mental health challenges, financial insecurity, loneliness, boredom, generational divides. This report has talked a lot about ensuring that the response to APP fraud is integrated in the UK's broader fraud response, and that integrated within a broader approach to economic crime. Ultimately tackling APP fraud requires integrating action into the Government's broadest efforts to address our deep-rooted societal challenges of which APP fraud is in many ways a symptom, rather than a cause.

Recommendations

- **Launch nationwide campaigns to raise awareness of scam tactics,** particularly those leveraging AI and social media.
- **Ensure there is awareness and understanding of the upcoming Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS)**.
- **Employ an 'educate from all angles approach',** working with partners, experimenting with medium, forum, and messaging, including working with schools to ensure fraud education starts from a young age.
- **Mandate FCCRAS to prioritise victims by offering clear process insights,** regular updates, and reassurance alongside enhanced law-enforcement support.
- **Boost awareness and access to existing help services** (e.g. Victim Support) and expand regional, face-to-face support for fraud victims.
- **Prevent repeat victimisation** through tailored training, dedicated resources, and ongoing guidance for those who've already suffered fraud.
- **Actively support those exhibiting characteristics of vulnerability to fraud** and work cross-department to address the systemic roots of fraud vulnerability.

---

[1] As committed to in the Economic Crime Plan 2023-26

[2] Following this, Georgian authorities froze the assets of key figures involved in in the call centres, demonstrating the invaluable role of investigate journalism in exposing organised fraud.

[3] See the APPG on Fair Banking and APPG on Anti-Corruption's Economic Crime Manifesto 2 for further information on how the UK can fight illicit financial flows.

Conclusion

APP fraud leaves a trail of devastation in its wake. It poses a threat to national security, economic prosperity, and psychological wellbeing. APP fraud ruins lives and steals wealth around the world. The time for Government action is now.

The Mandatory Reimbursement Requirement is a crucial initial step in protecting consumers from the sharpest edges of fraud and, following the 'lost decade' of fraud response, represents the UK Government's renewed focus. Early evidence suggests the MRR may be having its intended impact, with reimbursement increasing, and payment service providers investing considerably into prevention. The independent one-year review will be essential in assessing the impact of the MRR and whether further steps are necessary to close reimbursement gaps, promote consistency, and enhance data sharing.

The MRR alone is insufficient in beating back the rushing tide of fraud, however, and steps must be taken to better share the costs responsibilities of protection and prevention. There can be no half measures in tackling a problem of this scale that operates cross-border and at the cutting edge of technology.

The commitment of the new Government to issue an updated Fraud Strategy is a vital opportunity to develop a 'no half measures', holistic approach to tackling APP fraud. The recommendations included in this report, if included in the updated fraud strategy, would form the backbone of such an approach. It would:

- **Close remaining gaps in reimbursement**
- **Incentivise investment in prevention**
- **Equip and reform law enforcement to provide a real deterrent to fraud**
- **Tackle the problem at source through international collaboration**
- **End the UK's role as an enabler of fraud**
- **Foster a fraud resilient population**

This would amount to a world-leading approach to counter-fraud that is:

- **Ambitious –** setting bold goals, expanding reimbursement, prevention, data-sharing, enforcement and education at scale.
- **Collective –** enlisting every stakeholder – from government, regulators, and law enforcement to financial institutions, crypto firms, tech platforms and the public.
- **Collaborative –** breaking down silos, fostering cross-sector and international partnerships to share intelligence, coordinate operations and align incentives.
- **Comprehensive –** covering the full fraud lifecycle – prevention, detection, redress, deterrence and victim support, and using every tool and tactic to achieve them.
- **Fair –** distributing obligations and liabilities proportionately, ensuring no group bears an undue burden.
- **Integrated –** ensuring APP fraud measures are viewed as one manifestation of a broader problem, integrated within the broader Fraud Strategy, Economic Crime Plan, international efforts, whilst recognising cross-departmental dependencies.
- **Agile –** equipping the collective response and building in mechanisms for rapid adaptation to emerging threats and new technologies, whilst investing in and adopting leading-edge technologies to stay ahead of the curve.

The UK can lead the fight against APP fraud. The recommendations in this report provide the blueprint for the Government to do so.

Recommendations longlist

Recommendations for the independent review of the Mandatory Reimbursement Requirement, and PSR actions.

The APPG recommends that the independent one-year review and ongoing evaluation of the MRR, considers and undertakes the following measures:

- **Consumer focussed survey** to understand the awareness of the MRR, its impact on increasing trust and confidence, as well as customer experience across the reporting and claims process.
- **Understand whether reports of fraud gone up**, and if not, is that due to improved fraud prevention or a lack of awareness of the MRR?
- **Engage with the Financial Ombudsman Service** to understand the experience of customers whose complaints are not resolved or disputed under the terms of the MRR, and to understand how many claims over £85,000 were successfully reimbursed after going to FOS.
- **Engage with PSPs to understand how they are implementing the MRR,** especially in terms of how 'consumer standard of caution' is applied, as well as where cases have been deemed a 'civil dispute'.
- **Engage with PSPs to better understand the steps they have taken to improve detection and prevention,** in order to assess whether further guidance, standards and support should be introduced in these areas, in collaboration with the Lending Standards Board.
- **Examine what difficulties smaller PSPs and non-signatories of the CRM have faced** in preparing for and implementing the MRR?
- **Closely examine whether the MRR is inadvertently shifting fraud elsewhere,** and if so where, including looking outside the PSR's remit to cryptocurrency.

Based off the review, the PSR should:

- **Closely examine whether further regulation is necessary** to include International Bank Transfers, Credit Unions, Municipal Banks, or National Savings Banks that don't participate in the Faster Payment Scheme.
- **Assess whether the £85,000 reimbursement limit should be reviewed.**

Additionally, the PSR should consider:

- **Whether to mandate data sharing on a statutory footing,** and what this would take in terms of infrastructure and capabilities.

Recommendation for the Fraud Strategy

The upcoming Fraud Strategy should commit to the following:

Closing the gaps in reimbursement

- **Consider expanding the MRR to cover fiat-to-crypto transfers over UK payment systems,** (pending the judgements of the independent one-year review of the MRR) so that both sending PSPs and crypto deposit receivers share liability under the 50:50 cost-share model.
- **Fraud prevention should be a core part of the government's future regulation strategy for crypto,** including gathering data on the volume and value of fraud taking place across their platforms, and improving customer education on their platforms.
- **Consider introducing a mandatory reimbursement requirement for international transfers and remittance services,** (pending the judgements of the independent one-year review of the MRR), obliging PSPs to reimburse victims of APP fraud on cross-border transactions, enforced by the FCA.
- **Commit to maintain the FOS' 'fair and reasonable' remit** to ensure consumers harmed by novel or unregulated scams – such as those involving cryptocurrency or cross-border transfers – have access to redress when rigid rules fall short.
- **Commit to increasing funding of the FOS,** so that it is better equipped to handle the quantity of cases it receives.
- **Legislate to create a specialist Financial Services Tribunal,** empowering it to deliver swift, expert adjudication and binding precedent for complex and high-value financial disputes beyond the scope of the FOS. In the meantime, complex cases should remain within FOS remit.

Renewed attention on fraud towards business

- **Renewed focus on the impact of fraud on businesses,** and what can be done to better protect businesses from fraud and support them in prevention efforts.

Putting prevention at the strategic heart of counter-fraud

- **Introduce a tech levy** to raise vital funds for the counter-fraud response.
- **Scope possibility for reimbursement cost-sharing** between financial institutions and those responsible for enabling fraud.
- **Mandate action by social media firms** by placing the Online Fraud Charter on statutory footing.
- **Bring forward the implementation of the Online Safety Act,** and strengthen Code of Conduct for fraudulent content.

Providing an effective deterrent to fraud

- **Commit to providing stable core funding for fraud policing,** which is ring-fenced and multi-year, in line with policing for other national security threats.
- **Establish an Economic Crime Fighting Fund** to support funding for fraud policing.
- **The City of London Police should function as a single command structure,** acting as the policing lead for economic crime, setting a national policing strategy, with ringfenced assets at the regional tier of policing.
- **Fund a stronger network of Regional Economic Crime Hubs** to proactively investigate complex cyber-enabled fraud, with the aim to develop Regional Economic Crime Super Hubs in the future.
- **Policing should prioritise a 'quality' over 'quantity' approach,** focussing on more targeted police operations and 'online and upstream' interventions.
- **Consider how the model of the dedicated Central London Economic Crime Court can be expanded across regions**.
- **Revise sentencing guidelines** to reflect the societal harms of fraud.

Enabling prevention through data sharing

- **Enable data sharing through a centralised platform** to coordinate cross-sector intelligence, standardise practices, and enable real-time collaboration across the fraud prevention ecosystem.
- **Provide clear, practical guidance on how data sharing is GDPR compliant** to ensure legal certainty and compliance.

A global response to a global problem

- **Formalise international partnerships,** including negotiating bilateral MOUs with foreign law-enforcement agencies, financial intelligence units, and regulators to enable secure, real-time data, evidence and intelligence sharing.
- **Deploy technical assistance to 'source' countries** to build capacity in high-risk jurisdictions.
- **Focus on high-impact interventions,** targeting the "arteries" of organised fraud through joint task forces and precision enforcement – rather than broad, low-yield cooperation – to disrupt the most harmful networks.
- **Elevate China as a strategic partner,** making diplomatic engagement with China a priority, leveraging its regional influence and recent domestic anti-scam actions to tackle cross-border scam operations.
- **Champion a global coalition,** building on the Global Fraud Summit by spearheading an international architecture or "coalition of the willing" to drive a unified, UK-led approach to fraud prevention and victim protection.
- **Lead on establishing international fraud architecture,** by working to establish an equivalent body to FATF that oversees and coordinates international counter-fraud efforts.

Ending the enabling role of the UK

- **The strategy should recognise that solving fraud requires a focus on the onward laundering of fraud proceeds**, *and ensure it focusses on the problem of fraud from end to end, recognising the role the government has to play at each stage.*
- **Ensure the strategy is adequately integrated into the broader Economic Crime agenda** and working cross-department to end the UK's role as an enabler of fraud.

Building a fraud resilient population

- **Launch nationwide campaigns to raise awareness of scam tactics,** particularly those leveraging AI and social media.
- **Ensure there is awareness and understanding of the upcoming Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS)**.
- **Employ an 'educate from all angles approach',** working with partners, experimenting with medium, forum, and messaging, including working with schools to ensure fraud education starts from a young age.
- **Mandate FCCRAS to prioritise victims by offering clear process insights,** regular updates, and reassurance alongside enhanced law-enforcement support.
- **Boost awareness and access to existing help services** (e.g. Victim Support) and expand regional, face-to-face support for fraud victims.
- **Prevent repeat victimisation** through tailored training, dedicated resources, and ongoing guidance for those who've already suffered fraud.
- **Actively support those exhibiting characteristics of vulnerability to fraud** and work cross-department to address the systemic roots of fraud vulnerability.

Bibliography

Cifas [2024]. How could the Payment Systems Regulator's mandatory reimbursement impact fraud? Three questions from the counter-fraud industry. Retrieved from https://www.cifas.org.uk/insight/fraud-risk-focus-blog/psr-rule-reimbursement-impact

UK Government [2025]. APP scams Evaluation Consultancy – Find a Tender. Retrieved from https://www.find-tender.service.gov.uk/Notice/032384-2025

UK Finance [2025]. Annual Fraud Report 2025. Retrieved from https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2025

Home Office [2025]. Lord Hanson unveils ambitious new approach to tackling fraud. Retrieved from https://www.gov.uk/government/news/lord-hanson-unveils-ambitious-new-approach-to-tackling-fraud

All Party Parliamentary Group on Fair Banking [2025]. Authorised Push Payment Fraud – Who Bears the Burden? Retrieved from https://www.appgbanking.org.uk/s/APP-Fraud-report-2025.pdf

National Trading Standards [2023]. 19 million lose money to scams but fewer than a third report. Retrieved from https://www.nationaltradingstandards.uk/news/19-million-lose-money-to-scams-but-fewer-than-a-third-report/

The Economist [2025]. The vast and sophisticated enterprise that is Scam Inc. Retrieved from https://www.economist.com/leaders/2025/02/06/the-vast-and-sophisticated-global-enterprise-that-is-scam-inc

PSR [2023]. PSR publishes first APP scams performance report. Retrieved from https://www.psr.org.uk/news-and-updates/latest-news/news/psr-publishes-first-app-scams-performance-report/

UK Finance [2023]. Criminals steal over half a billion pounds and nearly 80 per cent of APP fraud starts online. Retrieved from https://www.ukfinance.org.uk/news-and-insight/press-release/criminals-steal-over-half-billion-pounds-and-nearly-80-cent-app

UK Finance [2021]. Criminals exploit Covid-19 pandemic with rise in scams targeting victims online. Retrieved from https://www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-pandemic-rise-scams-targeting-victims-online

NCA [n.d.]. Fraud – National Crime Agency. Retrieved from https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

Reuters [2021]. Insight: Welcome to Britain, the bank scam capital of the world. Retrieved from: https://www.reuters.com/world/uk/welcome-britain-bank-scam-capital-world-2021-10-14/

Wikipedia [n.d.]. Crime in Singapore. Retrieved from https://en.wikipedia.org/wiki/Crime_in_Singapore

GASA [2024]. Singapore's Shared Responsibility Framework: A Global Model for Combating Phishing Scams. Retrieved from https://www.gasa.org/post/singapore-s-shared-responsibility-framework-a-global-model-for-combating-phishing-scams

Info communications Media Development Authority [2025]. Anti-Scam Measures. Retrieved from https://www.imda.gov.sg/how-we-can-help/anti-scam-measures

Crowe UK [2023]. Annual Fraud Indicator. Retrieved from https://www.crowe.com/uk/insights/annual-fraud-indicator

PSR [2016]. Which? super-complaint: Consumer safeguards in the market for push payments. Retrieved from https://www.psr.org.uk/media/t0sln5vn/which-super-complaint-sep-2016.pdf

PSR [2022]. APP Scams: Requiring Reimbursement. Retrieved from https://www.psr.org.uk/media/kzlncenx/psr-cp22-4-app-scams-reimbursement.pdf

Lending Standards Board [2024]. CRM Code for Authorised Push Payment fraud winds down having more-than trebled reimbursement rates, slashed average losses, and slowed scam growth. Retrieved from https://www.lendingstandardsboard.org.uk/crm-code-for-authorised-push-payment-fraud-winds-down-having-more-than-trebled-reimbursement-rates-slashed-average-losses-and-slowed-scam-growth

PSR [2024]. Authorised Push Payment (APP) scams performance report. Retrieved from https://www.psr.org.uk/media/y0tbscjh/app-fraud-performance-report-covering-2023.pdf

Lending Standards Board [2020]. Thematic Review of Effective Warnings (Contingent Reimbursement Model Code). Retrieved from https://www.lendingstandardsboard.org.uk/wp-content/uploads/2020/12/Thematic-review-of-Effective-Warnings-1.pdf

UK Finance [2024]. Annual Fraud Report 2024. Retrieved from https://www.ukfinance.org.uk/system/files/2024-06/UK%20Finance%20Annual%20Fraud%20report%202024.pdf

PSR [2024]. PS24/7: Faster Payments APP scams reimbursement requirement: Confirming the maximum level of reimbursement. Retrieved from https://www.psr.org.uk/media/e30pwlly/ps24-7-app-scams-maximum-level-of-reimbursement-policy-statement-oct-2024.pdf

Lending Standards Board [2024]. The new rules for Authorised Push Payment fraud reimbursement – and what they mean for scam prevention. Retrieved from https://www.lendingstandardsboard.org.uk/the-new-rules-for-authorised-push-payment-fraud-reimbursement-and-what-they-mean-for-scam-prevention/

Financial Times [2025]. Is the UK failing victims of fraud? Retrieved from https://www.ft.com/content/964d2ffc-804c-4016-8c90-814fec68ecb8?

PSR [2023]. PS23/4: Fighting authorised payment scams: final decision. Retrieved from https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf

NICE Actimize [2023]. PSR's New Rules for Reimbursement Will Impact More PSPs. Retrieved from https://www.niceactimize.com/blog/fraud-prevention-psrs-new-rules-for-reimbursement-will-impact-more-psps/

Reuters [2024]. FCA signals watchdog open to ending to free banking Britain. Retrieved from https://www.reuters.com/business/retail-consumer/consumer-duty-rules-could-reduce-levies-fca-ceo-says-2024-03-14/

PSR [2024]. CP22/4: Authorised push payment (APP) scams: Requiring reimbursement. Retrieved from https://www.psr.org.uk/publications/consultations/cp22-4-app-scams-requiring-reimbursement/

Cifas [2024]. Tackling financial crime through enhanced data sharing: The key to preventing APP scams. Retrieved from https://www.cifas.org.uk/insight/fraud-risk-focus-blog/data-sharing-tackle-financial-crime-app-scams

PSR [2023]. PS23/3 Annex 4: Fighting authorised push payment fraud: A new reimbursement requirement. Retrieved from https://www.psr.org.uk/media/ycpd2ogg/ps23-3-annex-4-cost-benefit-analysis-june-2023.pdf

UK Finance [2024]. Over £570 million stolen by fraudsters in the first half of 2024. Retrieved from https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps570-million-stolen-fraudsters-in-first-half-2024

PSR [2023]. PS23/3: Fighting authorised push payment fraud: a new reimbursement requirement. Retrieved from https://www.psr.org.uk/media/rxtlt2k4/ps23-3-app-fraud-reimbursement-policy-statement-june-2023.pdf

Pay UK [2024]. FPS Reimbursement Rules: Compliance Monitoring Regime. Retrieved from https://www.wearepay.uk/wp-content/uploads/2024/09/FPS-Reimbursement-Rules-Compliance-Monitoring-Regime-v5.0.pdf

PSR [2024]. International Fraud Awareness Week: PSR research shows reimbursed fraud victims feel more vigilant about fraud risks, not less. Retrieved from https://www.psr.org.uk/news-and-updates/latest-news/news/international-fraud-awareness-week-psr-research-shows-reimbursed-fraud-victims-feel-more-vigilant-about-fraud-risks-not-less/

Fintech Finance News [2025]. What percentage of customers leave their bank after an incident of APP fraud? Retrieved from https://ffnews.com/thought-leader/whitepaper/what-percentage-of-customers-leave-their-bank-after-an-incident-of-app-fraud-aci-worldwide/

FSCS [2023]. Beyond Compensation: The Role of FSCS in Raising Consumer Trust and Confidence in the UK Financial Services Industry. Retrieved from https://www.fscs.org.uk/globalassets/industry-resources/research/202312-fscs-beyond-compensation-fscs-final.pdf

Which? One in five fraud victims send money to criminals via cryptocurrency. Retrieved from https://www.which.co.uk/news/article/one-in-five-fraud-victims-send-money-to-criminals-via-cryptocurrency-alCPq3K8KPa8

Wealth Recovery Solicitors [2024]. New PSR rules for app fraud reimbursement and implications for crypto-fraud. Retrieved from https://wealthrecovery.co.uk/resources/new-regulator-rules-for-fraud-reimbursement/

FCA [2025]. DP25/1: Regulating cryptoasset activities. Retrieved from https://www.fca.org.uk/publications/discussion-papers/dp25-1-regulating-cryptoasset-activities

FCA [2025]. FCA seeks feedback on regulation of cryptoasset trading platforms in next phase of road to regulation. Retrieved from https://www.fca.org.uk/news/press-releases/fca-seeks-feedback-regulation-cryptoasset-trading-platforms

FCA [n.d.]. Crypto Roadmap. Retrieved from https://www.fca.org.uk/publication/documents/crypto-roadmap.pdf

HM Treasury [2025]. New Approach to Ensure Regulators and Regulation Support Growth. Retrieved from https://www.gov.uk/government/publications/a-new-approach-to-ensure-regulators-and-regulation-support-growth/new-approach-to-ensure-regulators-and-regulation-support-growth-html

All Party Parliamentary Group on Fair Banking [2023]. Building a Framework for Compensation and Redress. Retrieved from https://www.appgbanking.org.uk/s/Redress-Report-2023-230217-Web.pdf

Law Gazette [2019]. Room to Grow. Retrieved from https://www.lawgazette.co.uk/features/room-to-grow/5106201.article

Home Office [2023]. Fraud Strategy: Stopping Scams and Protecting the Public. Retrieved from https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf

PSR [2024]. New report from PSR shows how fraudsters exploit major platforms to scam consumers. Retrieved from https://www.psr.org.uk/news-and-updates/latest-news/news/new-report-from-psr-shows-how-fraudsters-exploit-major-platforms-to-scam-consumers/

Which? [2024]. A Year On from the Online Fraud Charter. Retrieved from https://www.which.co.uk/policy-and-insight/article/a-year-on-from-the-online-fraud-charter-aefBu4h2Pre8

Meta [2025]. Meta Reports Fourth Quarter and Full Year 2024 Results. Retrieved from https://investor.atmeta.com/investor-news/press-release-details/2025/Meta-Reports-Fourth-Quarter-and-Full-Year-2024-Results/

UK Finance [2024]. Building a Better Society: A financial services manifesto for the UK. Retrieved from https://www.ukfinance.org.uk/system/files/2024-05/Building%20a%20Better%20Society%20-%20A%20financial%20services%20manifesto%20for%20the%20UK_1.pdf

Cifas & GASA [2024]. State of Scams UK 2024. Retrieved from https://www.gasa.org/_files/ugd/7bdaac_bc34e713c6434551a9c8f25207e1be9d.pdf

Home Affairs Committee [2025]. New inquiry: Harnessing the potential of new forms of digital ID. Retrieved from https://committees.parliament.uk/committee/83/home-affairs-committee/news/207446/new-inquiry-harnessing-the-potential-of-new-forms-of-digital-id/

Which? [2025]. Which? comments ahead of new duties to prevent user-generated fraud under the Online Safety Act coming into effect on 17th March. Retrieved from https://www.which.co.uk/policy-and-insight/article/which-comments-ahead-of-new-duties-to-prevent-user-generated-fraud-under-the-online-safety-act-coming-into-effect-on-17th-march-aNMlI3D7RMxx

Ofcom [n.d.]. Quick guide to illegal content codes of practice. Retrieved from https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/codes-of-practice

Australian Government Treasury [2025]. Scam Prevention Framework – Protecting Australians from scams. Retrieved from https://treasury.gov.au/publication/p2025-623966

Fraud Act 2006 and Digital Fraud Committee [2022]. Fighting Fraud: Breaking the Chain. Retrieved from https://committees.parliament.uk/publications/31584/documents/177260/default/

Financial Times [2023]. Meta expands data to accord with UK banks in push to cut online fraud. Retrieved from https://www.ft.com/content/ff5ed0ed-170d-4439-a789-d658936fd5f5

RUSI [2024]. War Fraud: How the UK Can Step Up to the 21st Century Crime Wave. Retrieved from https://www.rusi.org/explore-our-research/publications/commentary/war-fraud-how-uk-can-step-21st-century-crime-wave

Innovate Finance [2025]. A Technology Strategy to Smash Fraud. Retrieved from https://ww2.innovatefinance.com/wp-content/uploads/2025/04/a-technology-strategy-to-smash-fraud-04.04.25.pdf

RUSI [2024]. Towards a New Model for Economic Crime Policing: Target 2030. Retrieved from https://www.rusi.org/explore-our-research/publications/special-resources/towards-new-model-economic-crime-policing-target-2030

ICO [2024]. Data protection is not an excuse when tackling scams and fraud. Retrieved from https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/data-protection-is-not-an-excuse-when-tackling-scams-and-fraud/

Which? [2023]. Sharing data to tackle fraud. Retrieved from https://media.product.which.co.uk/prod/files/file/gm-b5149f39-09aa-425f-94df-ee2ca19d197f-data-sharing-policy-report-nov-23.pdf

ICO [n.d.]. Sharing personal information when preventing, detecting and investigating scams and frauds. Retrieved from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/sharing-personal-information-when-preventing-detecting-and-investigating-scams-and-frauds/

UK Parliament [2024]. Data Use and Access Bill 2023-24. Retrieved from https://publications.parliament.uk/pa/bills/cbill/59-01/0199/240199.pdf

Cifas [2024]. Scammers stole £11.4 billion from UK people in last 12 months. Retrieved from Scammers stole £11.4 billion from UK people in last 12 months | Cifas

Justice Committee [2024]. Justice Response Inadequate to Meet Scale of Fraud Epidemic. Retrieved from https://committees.parliament.uk/committee/102/justice-committee/news/173618/justice-response-inadequate-to-meet-scale-of-fraud-epidemic/

Cifas [2024]. Cifas challenges government to do more to tackle fraud epidemic. Retrieved from https://www.cifas.org.uk/newsroom/fraud-pledges-2024

Spotlight on Corruption [2024]. Spotlight calls for Economic Crime Fighting Fund, after budget small change. Retrieved from https://www.spotlightcorruption.org/spotlight-economic-crime-fighting-fund/

The Week [2024]. How Scotland Yard Took Down iSpoof in UK's biggest ever fraud investigation. Retrieved from https://theweek.com/news/crime/958634/how-scotland-yard-took-down-ispoof

Justice Committee [2022]. Fraud and the Justice System. Retrieved from https://committees.parliament.uk/publications/30328/documents/175363/default/

Home Affairs Committee [2021]. Written evidence submitted by DCI Steven Maloney, Tarian (FRA0006). Retrieved from committees.parliament.uk/writtenevidence/42088/html/

Cifas [2024]. The Cifas Fraud Pledges 2024. Retrieved from https://www.cifas.org.uk/secure/contentPORT/uploads/documents/Cifas%20Films/Fraud%20Pledge%20Full%20Document%20-%20Digital.pdf

The Guardian [2025]. Beatings, Torture and Electric Shocks: Freed Scam Compound Workers Allege Horrific Abuse. Retrieved from https://www.theguardian.com/world/2025/feb/25/beatings-torture-and-electric-shocks-freed-scam-compound-workers-allege-horrific-abuse#:~:text=In%20an%20interview%20with%20the,Karen%20Benevolent%20Army%20(DKBA).

OCCRP [2025]. Scam Empire: Inside a Merciless International Investment Scam. Retrieved from https://www.occrp.org/en/project/scam-empire/scam-empire-inside-a-merciless-international-investment-scam

NCA [2024]. Notorious Criminal Marketplace Selling Victim Identities Taken Down in International Operation. Retrieved from https://www.nationalcrimeagency.gov.uk/news/notorious-criminal-marketplace-selling-victim-identities-taken-down-in-international-operation

BBC News [2025]. How a viral post saved a Chinese actor from Myanmar's scam centres. Retrieved from https://www.bbc.co.uk/news/articles/cd606l1407no

BenarNews [2025]. Myanmar militia hosting scam centres says it will deport 8000 foreigners. Retrieved from https://www.benarnews.org/english/news/thai/myanmar-scam-centers-foreign-workers-02132025135909.html

RUSI [2024]. Professional Enablers of Financial System Abuses. Retrieved from https://www.rusi.org/explore-our-research/projects/professional-enablers-financial-system-abuses

IDnow [2024]. UK Fraud Awareness Report 2024. Retrieved from https://www.idnow.io/portfolio/2024-uk-fraud-awareness-report/

JT Global [2025]. Consumers Unaware of the Risks Posed by Authorised Push Payment Fraud. Retrieved from https://blog.international.jtglobal.com/consumers-unaware-of-the-risks-posed-by-app-fraud

The Times [2025]. Scam refunds must not distract from detection and prevention. Retrieved from https://www.thetimes.com/uk/law/article/app-push-payment-fraud-scams-detection-prevention-comment-pjktpnpm5

All Party Parliamentary Groups on Fair Banking and Anti-Corruption & Responsible Tax [2024]. Economic Crime Manifesto II. Retrieved from https://www.appgbanking.org.uk/s/Economic-Crime-Manifesto-2024-Digital-1704.pdf

Take Five to Stop Fraud [n.d.]. Retrieved from https://www.takefive-stopfraud.org.uk/

Open University [n.d.]. Scam Interceptors. Retrieved from https://connect.open.ac.uk/science-technology-engineering-and-maths/scam-interceptors/

FCA [n.d.]. What Do Firms Do to Educate Their Customers? Retrieved from https://www.fca.org.uk/data-visualisation/3-what-do-firms-do-educate-their-customers

Hack For Public Good [2025]. Unpacked Experience. Retrieved from https://www.hack.gov.sg/2025/unpacked

Singapore Police Force [2024]. How migrant workers and migrant domestic workers fought scams through an anti-scam TikTok challenge! Retrieved from https://www.police.gov.sg/Media-Room/Police-Life/2024/04/Tiktoking-to-Raise-Scam-Awareness

TikTok Newsroom [2024]. TikTok Launches Scam Prevention Edition of Its Digital Wellness Hub to Help Users Navigate Online Scams. Retrieved from https://newsroom.tiktok.com/en-sg/tiktok-launches-scam-prevention-edition-of-its-digital-wellness-hub-to-help-users-navigate-online-scams

Cifas [n.d.]. Anti-Fraud Lesson Plans. Retrieved from https://www.cifas.org.uk/insight/public-affairs-policy/anti-fraud-lesson-plans

Public Accounts Committee [2024]. Progress combatting fraud. Retrieved from https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/40/report.html#:~:text=The%20Department%20acknowledges%20that%20the,set%20up%20to%20tackle%20fraud.

Victim Support [n.d.]. Retrieved from https://www.victimsupport.org.uk/

City of London Police [2021]. First time victims of fraud go on to lose £373 million to repeat frauds – with victims of at least one investment fraud worst affected. Retrieved from https://www.cityoflondon.police.uk/news/city-of-london/news/2021/march/first-time-victims-of-fraud-go-on-to-lose-373-million-to-repeat-frauds/?s=04

FCA [2023]. Financial Lives Survey 2022. Retrieved from https://www.fca.org.uk/publications/financial-lives/financial-lives-survey-2022-key-findings?utm

Wired [2024]. The Loneliness Epidemic is a Security Crisis. Retrieved from https://www.wired.com/story/loneliness-epidemic-romance-scams-security-crisis/

appgbanking.org.uk

appg Fair Banking