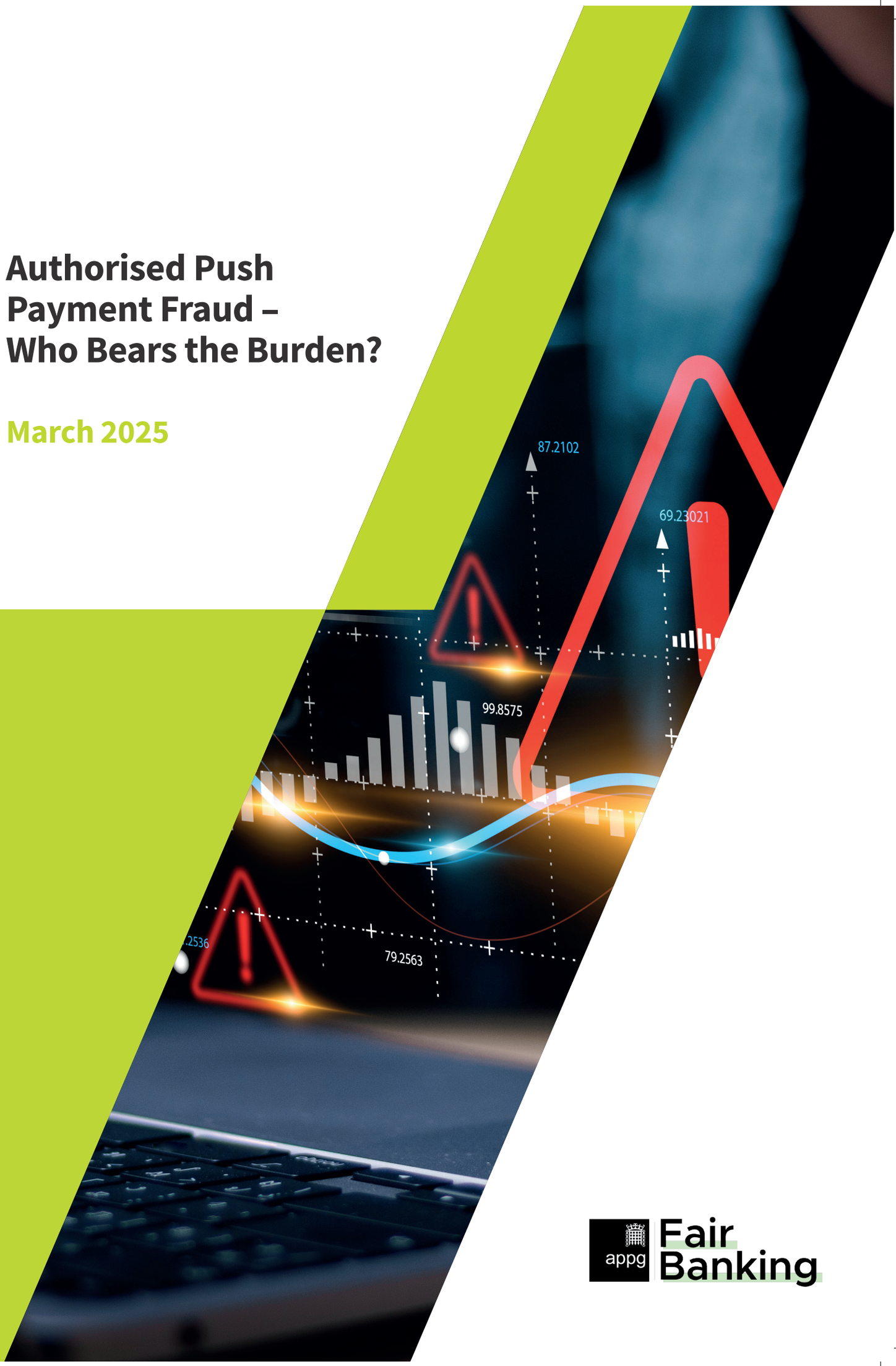
Authorised Push Payment Fraud – Who Bears the Burden?

March 2025



appg Fair Banking

Produced with the support of Richardson Hartley Law.

Disclaimer

This is not an official publication of the House of Commons or the House of Lords. It has not been approved by either House or its committees. All-Party Parliamentary Groups are informal groups of Members of both Houses with a common interest in particular issues. The views expressed in this report are those of the group.

Table of contents

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 Richardson Hartley Law

Richardson Hartley Law specialises in fraud recovery claims across the UK. It offers a no win, no fee service to help scam victims access justice to recover their lost funds.

The law firm has been set up by Martin Richardson, a solicitor with a proven track record in large volume litigation and Jonathan Hartley, a well-respected UK media consultant.

As well as providing scam recovery services, the solicitors practice also offers fraud prevention advice. With this in mind, the law firm operates under the trading name National Fraud Helpline which has an associated website (www.nationalfraudhelpline.co.uk) offering scam prevention help and the latest fraud news. National Fraud Helpline regularly appears in the media, highlighting the latest fraud trends and showcasing individual scams as a warning to others.

The stated aim of the law firm is to create anti-fraud products based on analysing the data it receives through the claims process. With this in mind, Richardson Hartley Law has teamed up with Artificial Intelligence firms to help create technological solutions to the growing problem of online fraud.

Richardson Hartley Law ultimately hopes to work alongside banks and other payment service providers to tackle the UK's 'scamdemic'.

About the author

Jonathan Russell, Director, Lacing Limited
jr@lacinguk.com

Jonathan is a former journalist who now works in research and media relations. Jonathan advises on a variety of different situations including litigation, investment and regulatory matters. He has worked with the APPG, informally, for a number of years, including on our De-Banking Report (2024).

Foreword

Consumers, regulators and the banking industry have made huge progress in tackling banking fraud in recent years. Biometric identification, two-factor authentication and transaction monitoring have all helped identify and prevent billions of pounds worth of fraud. Each step forward in this battle to beat the scammers is a double win - money kept out of the pockets of criminals and in the pockets of the rightful owners.

This progress, along with compensation schemes available to victims of fraud, demonstrate just how seriously all parties are taking this problem. It is impressive and deserves recognition. Without it, consumers would have been left exposed to unchecked criminality and faith in the financial system would have been further undermined.

But much still needs to be done. As we explore in the report, the annual losses to Authorised Push Payment (APP) fraud are much larger than had previously been estimated – amounting to billions of pounds rather than the hundreds of millions we have previously been told. It is also the case that while total sums lost to APP fraud are falling, on other measures we are losing the battle. Victims of romance scams, perhaps the most psychologically chilling of all these crimes, will make on average 10 payments before they, or their bank, realise they have been duped. This is twice the average number of payments that were being made just five years ago. While the rise in payments per case is more acute in romance scams than any other type of fraud, the metric is up across the board. On this measure our Payment Service Providers (PSPs), banks to you and me[1], are failing in the battle against fraudsters.

Equally this report provides some worrying early indications of how PSPs are responding to the new compensation scheme introduced in October last year. It is early days, but the indications are that banks are not processing compensation claims quickly enough, certainly not within the five-day deadline set by the payment regulator. Action should be taken on this. The compensation scheme has already been watered down once, the maximum payout reduced from £415,000 to £85,000 after extensive lobbying by the banks. It cannot be allowed to drift with victims left waiting for weeks or months for payouts they are due under the scheme. If there is a single overriding purpose of this report it is to keep minds and energies focused on the problem of fraud. We know that the fraudsters are working tirelessly to create new ways of scamming their victims. We need to do all we can to meet and exceed those levels of energy and productivity in response.

In our analysis we should not forget that the genesis of this problem does not lie with regulators, banks or consumers. It lies with the criminals, execrable individuals and organized crime gangs who have built an industry around targeting vulnerable people, stealing their money, their self-esteem, their trust, their confidence. Ultimately it is only by breaking the business model that we will resolve this problem, a cause we can all unite behind.

Introduction

Perhaps the best way to understand APP fraud is in simple business terms. For fraudsters to succeed they need a product, a route to market and a sales operation - the basic structure of any business. Their product, while fraudulent, must be convincing; fake identities backed up by social media profiles for romance scams; glossy brochures and websites for investment scams; forged documents and well-rehearsed sales pitches for property scams. The marketplace needs to be developed, where a 'mark' can be identified, engaged and then convinced to part with their cash. And, finally, that cash needs to be laundered, passed through a series of accounts, currencies and jurisdictions until it can be recycled back into the economy, shadow or otherwise.

All of this activity, while criminal, turns on the wheels of the established economy. Scams are devised using the same computers, telephones and offices that drive the bulk of the world economy; the marketplace for fraud is the social media platforms, messaging apps and telephony companies that all of us use on a daily basis; the money laundering takes place through the banks, fintech companies and cryptocurrency exchanges that plumb the global financial system.

This co-existence of the legitimate and the larcenous in the mainstream economy, while clearly a problem, is also an opportunity, presenting the best way of tackling the problem. Deprive anyone of the tools of their trade and you hit their productivity, slowing down activity and introducing costs that can make the activity unprofitable at best, less attractive at worst. This is what we are aiming at, harnessing the power of all organisations that form part of the fraudsters supply chain to stamp out the problem.

It may be argued that it is not the role of the private sector to police wrongdoing. Superficially this is true, however it is also true that it is not open to the private sector to look away, or even profit, from crime. Transaction charges, service fees, commission payments and advertising revenues do not differentiate between the dark and the light. Undetected and unchallenged, criminal activity boosts revenue for legitimate companies in the same way as lawful activity does. For this reason, if for no other, social media companies, banks and telecoms providers have a clear and unambiguous responsibility to tackle the problem of fraud, APP and other.

While the focus of this report is on protection and reimbursement rather than prosecution we should not ignore the role of law enforcement. Notwithstanding some recent successes it is indisputable that we are not doing nearly enough to catch these criminals. National Trading Standards estimate that 40 million people in the UK have been targeted by fraudsters, with some 35% of us going on to lose money. The bulk of these crimes are not reported to the police or other relevant authorities. Depressingly, this failure to report is almost inevitable in circumstances where the chances of successful prosecution are vanishingly small. A 2022 report[2] by the Justice Committee found that only 2% of police funding is dedicated to combating fraud, despite it accounting for over 40% of all reported crime. Much more work needs to be done on deterrence, a subject the APPG will return to as part of its broader focus on fraud in the banking system.

Scale of the problem

Establishing the scale of the fraud 'scamdemic' infecting the UK is no easy task. Action Fraud, the Payment Services Regulator (PSR)[3], UK Finance and others have all tried to pin down this shadow. Their numbers are insightful, not so much for what they tell us about the overall picture, but about the direction of travel, how fraud is changing; adapting to target parts of the economy that demonstrate the most vulnerability.

The two most relevant studies into APP fraud are from UK Finance and the PSR, both drawing from data provided by the banking industry. Broadly speaking, the studies paint a similar picture, UK Finance reporting 232,429 cases of APP fraud and losses of £459.7m in 2023 while PSR had 252,600 cases and losses of £341m. The divergence between these numbers is not wholly unexpected. UK Finance draws its data from its membership of 300 or so firms; the PSR numbers come from data provided by the 14 largest banking groups in the UK. The other factor is that they are both chasing shadows. Fraud is an exercise in deception. Success depends on the victim and their bank being hoodwinked. By definition neither know what is going on. This is certainly true at the outset of any fraud, and even when suspicion does arise there can be a temptation from both bank and customer to ignore the issue or categorise it as something other than what it really is.

In these circumstances all parties accept the real scale of APP fraud is much larger than the figures reported above. Trying to establish a more reliable figure we asked UK Finance and the PSR for their views about the true scale of the issue. UK Finance pointed us towards a survey conducted by Trading Standards which noted that only around a third of fraud victims report the crime to law enforcement or their bank. If this is correct then UK Finance's measure of fraud, £459.7m would indicate an underlying problem equating to £1.4bn.

This picture could be much worse though. The National Crime Agency estimates that 86% of frauds go unreported. Applying this multiplier to the UK Finance figure and you get to a total of £3.3bn in 2023.

The figures are startling and suggest the problem of APP fraud is far bigger than we thought. There is a significant gap though between £1.4bn and £3.3bn. To try and understand which end of this scale we should land when estimating the size of APP fraud we took a third metric, produced by anti-fraud group, CIFAS. In September 2023 the body concluded[4] that approximately £7.5bn was stolen from Britons over the proceeding 12 months through banking fraud. This figure encompassed all types of banking fraud. However it is possible to narrow this down to APP fraud using the PSR's metric that 40% of banking fraud are APP scams. Applying this metric gives a figure for APP fraud of £3bn in 2023.

While no more than an estimate, this figure is likely to be more representative of the scale of the problem than the much lower figures reported by UK Finance and the PSR. This is not to criticise their data. Both organisations accept that their figures only deal with reported fraud and do not cover the entire industry so fail to capture the full extent of the problem. The problem is significant, but so is the opportunity. The money lost to fraud is money lost not just to victims but to the entire economy. Given the Government's current push for economic growth, plugging this £3bn shaped hole in the UK economy is a clear and obvious priority.

The human cost

While £3bn is a big number, it tells a very small part of the story of APP fraud. A victim of the crime, someone who has suffered the cold-sweat of realising they have lost money to a scam, will care very little for the big picture. They will be more concerned about working out what has happened, what can be done and whether they can get their money back. They will then have the awful moment of realising they are going to have to tell their loved ones and dependants about their loss.

The emotional and psychological trauma of falling victim to fraud, particularly APP fraud with its insidious mechanisms of control, can be so severe it has been likened to domestic abuse. Academic studies[5] have found the same techniques of manipulation and control take place in both scenarios, with the victims subject to distortion of power and reality, their emotions manipulated and confidence undermined. Fraudsters will work to isolate their victims, imposing a code of secrecy on the relationship, before deliberately belittling them, often using shame to extract more cash. Friendships and families are negatively impacted, loneliness deepens, mental health degrades. For this reason, it is important we look through the economic scale of this crime to the people at the heart of the problem. APP Fraud is a nasty crime, as Richard Mbombo's case[6] demonstrates so painfully.

> *Richard Mbombo, a father of four, was holding down two cleaning jobs when he was conned out of nearly £10,000 by crypto scammers. Richard's ordeal began when he saw an advert on Facebook promising big returns on cryptocurrency, apparently backed by the PM, Sir Keir Starmer.*
>
> *He said: "I don't gamble, I don't even play the Lottery, but when I saw it I thought 'there maybe a chance, let me try.'" He clicked through to the EvincoInvest website, filled out a form, and was contacted by a manager who promised him big returns on cryptocurrency investments. After initially investing just £170,, EvincoInvest opened a Revolut account for him and sent him a bank card.*
>
> *He said: "Everything seemed very genuine, I couldn't suspect anything wrong in what I was doing. After this lady sent me the card, she said 'you see, everything is working properly, you can withdraw the money on to that card."*
>
> *Richard did just that as a test, withdrawing £20 from his trading account and transferring the money into his Halifax account. "I thought 'OK, that's fine', it made me trust them," he added.*
>
> *A few days later, he was persuaded to invest more money, depositing £1,000 of his own savings into his trading account, but that wasn't enough for the scammers, who pressured him into taking out a £10,000 loan with MBNA. The money was paid into his*

Halifax account, where staff initially blocked his payment to EvincoInvest, and called him to ask if he trusted the recipient. Despite saying he did, the bank refused to make the payment and locked his account for 24 hours.

The fraudsters then sent him details of a different bank account in the name of 'Gemma Croote', and coached him on how to persuade the bank to make the transfer. Whatsapp messages show they told him to keep the payments below £5,000 to avoid triggering a security check, and how to dupe the bank. After transferring around £10,000 the bank again froze his account, leading Richard to do further checks online about EvincoInvest.

"In my break time at work I started looking online and started to see that this was a scam," he said. "There were many people on Google complaining about this investment company.

"On that day, I knew these people had taken my money. I asked them to refund my money, but she said at that investment stage they could not refund.

"The following day I rode my motorbike to the address they had given me in the centre of London, but when I got there they didn't even know them." Richard said he felt "sick" when he realised he had been duped by fraudsters. A situation that was made even worse when the crooks turned increasingly aggressive as he tried to back out of his investment.

EvincoInvest staff wrote: "If you think your wife serves a man who cleans shit and doesn't want anything better than this, okay. You don't even get to spend time with your family because you clean someone else's place, it's a pity, you could achieve much more if you believed in yourself a bit more. You let everyone down, mo (sic) company, my colleagues, me, yourself, your future self mostly."

Richard has since stopped communicating with the company, and has been pursued a compensation claim through Richardson Hartley Law which has so far recovered £4,250 for him.

As demonstrated in this case study, it is not just how much money has been lost that matters. It is also the fact that someone deeply unpleasant has managed to inveigle their way into an unsuspecting person's life and trust. To do this the criminal needs direct contact with as wide a group of potential 'marks' as possible. Years ago this type of catfishing would have taken place in the small ads of a newspaper, a clumsy analogue approach to fraud. Now, with the advent of social media, fraudsters can get up close to their victims, conversing with thousands of people at once through mass mail outs and then targeting those who present as most vulnerable, and lucrative.

Fraud incubators

Perhaps the most startling statistic to have emerged from the APP fraud epidemic is one that sits outside the finance industry. Research by the PSR shows how social media and one company in particular sit at the heart of the fraud-ecosystem. Meta, and its platforms, Facebook, WhatsApp and Instagram, now provide the breeding ground for over half of all frauds in the PSR survey. Whether it is romance scams on WhatsApp, purchase scams on Facebook Marketplace or impersonation scams on Instagram, 54% of all scams start on a Meta platform, accounting for 18% of total losses to fraud.

It would be encouraging to be able to report firsthand what Meta is doing about the millions of pounds of fraudulent activity flowing across its platforms. We contacted Meta to ask them for their input on the problem and what they were doing. We got no response.

Digging into what the company has said publicly shows there is, at least, an awareness of the problem. In October last year the company announced[8] an information sharing partnership with UK banks, called the Fraud Intelligence Reciprocal Exchange, FIRE for short. Meta reported that an early stage trial, involving Metro Bank and NatWest, had resulted in 20,000 suspect accounts being shut down. While this is to be welcomed, it must be recognised that closing accounts is not the same as catching criminals. How much heat scammers are feeling from Meta's FIRE remains unclear. What we do know is that the scams keep coming, criminals exploiting the very personal and immediate communication channels that WhatsApp, Facebook and other platforms offer.

Case study

Max Greenhalgh, 19, was struggling to deal with his father's death in September 2023 when he was targeted by a scammer on Instagram. "I'd made a promise to myself that I was going to make my dad proud, and started my own business day trading on foreign exchange markets," he said, spending hundreds of hours researching the subject.

"The scammer reached out to me, offering mentorship and promising me crazy numbers if I worked with him. He offered to take me under his wing and blasted me with pictures of him travelling the world with his girlfriend, and with nice cars. I opened up to him about my dad, and shared all aspects of my life with him. He told me he'd help me make my dad proud. I trusted him so much - more than a mentor, he posed as my friend."

Over two weeks in January, Max ploughed £4,750 into a crypto wallet he believed he was funding but turned out to be a fake trading account set up by the scammer.

He described as "earth-shattering" the moment the fraudster came clean in a text message that read: "I'm sorry, I've done you dirty, this was all a lie and I'm keeping all the money. I hope life gives you the best of it, keep trading, you'll be amazing one day. I'm very sorry, you seem like a nice guy."

This case, and so many like it, demonstrate just how easy it is for criminals to exploit the hopes and dreams we all share. This is why it is crucial that social media companies are drawn into the heart of this battle, facing up to the same responsibilities and costs as the finance industry.

At the moment this is simply not the case. The regulatory and legislative burden placed on Meta and other social media platforms is nothing like that faced by the finance industry. In strict commercial terms, the incentives are all pushing the wrong way. Social media companies do not pay the price of compensating customers as PSPs do. The same goes for telecoms companies, the other key breeding ground for scams. This is a peculiar and unbalanced state of affairs and is something that generates significant frustration from the banking sector, as UK Finance explained:

> *Most fraud victims are identified, targeted, and exploited through social media platforms and mobile networks. Only the technology and telecommunications sectors can stop fraud at source. Online services must invest in fraud prevention and consumer protection in the way our industry does. The measure of success should be effectiveness rather than compliance alone. Implementing minimal protections to achieve compliance is not enough.*

Through UK Finance the banking industry is calling on Government and the technology sector to take tough measures to tackle fraud. These include:

- Requiring the technology and telecommunications sectors to contribute to the costs of protecting the public from these crimes, and reimbursing victims.
- Holding the technology and telecommunications sectors to account by publishing evidence of actions taken on fraud prevention and their effectiveness.
- Improving user verification on social media, particularly marketplaces and dating platforms. This would include introducing Know Your Customer (KYC) controls, or two factor verification, on all online marketplaces.
- Mandatory use of regulated secure payment options on all online marketplaces, or any other online service that involves payments. A good exemplar of this is eBay, which offers a money back guarantee where an eligible payment method is used.
- Proactive vetting of the most common type of advertisements used by criminals.
- Requirement to investigate and act on mass replicated messages, such as "mum, I've lost my phone, can you send me some money".

A lot more work is needed into the role social media platforms will need to play, and pay, when it comes to addressing the problem of APP fraud. This will require further research, something we intend to address in subsequent reports. However, some of these measures, such as the requirement to investigate mass replicated measures and vetting of scam ads, should be acted on immediately.

The extent to which fraud is proliferating on the internet is particularly stark when you compare it to the standards we operate to in the physical world. If 50% of any type of crime was being funnelled through a single physical location, a shop, warehouse or marketplace, we would expect it to be tackled immediately, with severe penalties for those deemed responsible. That these standards do not apply to the online world is something that needs to be addressed with urgency. UK Finance has called for platform operators such as Meta to contribute towards the reimbursement of victims of fraud and to contribute to the Economic Crime Levy. These measures would be an important step, but alone would not go far enough. The Online Fraud Charter 2023 set out measures to help prevent fraud while The Online Safety Act 2023 gave Ofcom power to fine social media platforms if they are found to be carrying fraudulent advertising.

Once again, these measures are to be welcomed. Once again, they do not go far enough. As UK Finance set out in its 2024 Annual Fraud Report[9]:

> *We believe it is inequitable for the financial services sector to bear the costs stemming from other sectors' failure to adequately address their own fraud or anti money laundering risks… To really move the dial, the commitments made in the Online Fraud Charter need to translate into concrete action across the tech sector. These commitments could also become a global benchmark, building on the UK's fraud summit and recognising the international nature of fraud and the work needed to tackle it.*

Government now needs to legislate so that social media platforms are held accountable for their success, or failure, in tackling all types of fraud. The first step is to use the Online Safety Act to fine those companies that fail to police illegal content on their sites, however it is highly likely legislators will have to go further and require social media companies to contribute positively to the fight against fraud as banks and PSPs do.

Other industry sectors should also be pulled into this net. Fraudsters are exploiting weaknesses in industries such as property to extract large sums from victims. While this type of crime is not as common as online fraud it cannot and should not be ignored, not least because the sums of money at stake are often very significant. Con artists also target students or financially vulnerable people, often those who have moved away from the family home for the first time or are struggling to meet rental payments.

> *Alma Talbot lost £20,000 in a sophisticated property scam that she argues should have been spotted by the agency that was offering the property for rent. The 20-year old student was lured into the scam with the offer of a 25% discount on the £2,000 a month rental for a flat in Elephant & Castle if she paid the full year's rent in advance. After doing all reasonable checks including looking into the landlord and reading over the paperwork she made two payments from her Monzo account, the first for £10,000 the second for £9,730. While the first went through uninterrupted the second was flagged as potential fraud, but was later authorised by the bank once it had inspected her contract.*
>
> *Unfortunately, just hours after she had made the payment, the property agency alerted her to a potential problem. The agency said it had found that the name of the landlord she was dealing with did not match the owner's name on the Land Registry records. What had happened was the conman had taken out a lease on the flat to give him access to the property. He had then produced forged documents to set himself up as a 'landlord' offering the flat back out on the market but asking for a lump sum payment up front.*

Follow the data

As explored above, the two best sources of data on APP Fraud are from the PSR and UK Finance. While neither dataset can capture the full extent of the problem, both provide a roadmap, identifying trends and helping us to understand where we are winning and losing in the battle against fraud.

Both UK Finance and the PSR headline their reports with the financial scale of fraud, detailing how losses to APP fraud have declined over recent periods. UK Finance reported a 5% fall in the total value of APP fraud between 2022 and 2023. The PSR had the fall at 12%. As a measure of the amount of money ending up in the pockets of criminals this has to be welcomed. However, consider what is happening to the victims and the picture is not quite as clearcut.

As the value of fraud fell across the period, the number of cases rose. On UK Finance numbers cases were up 11% to 232,429; the PSR numbers were up 12% to 252,626. This discrepancy, with overall values dropping while frequency increases, is explained by a decrease in the cost of each case, fraudsters making off with less money for each victim they scam, a fall of 18%.

While it would be tempting to interpret this fall in the value of each case as a sign of progress, the reality is likely to be more mundane and down to the economic reality we have all been living through. As the cost-of-living squeeze came on during 2022 and 2023 ready cash dwindled, leaving people with less money to spend on everything, including as it turns out, scams.

This theory is backed up by the latest figures from UK Finance covering the first half of 2024. As the inflationary squeeze receded over this period, leaving people with more money to spend, so the value of each APP case rose again, hitting £2,195 over the first six months of the year, an increase of 16%.

What this analysis suggests is that to track criminal activity it is better to look at the number of cases rather than their value. On this measure the overall trend is not good, case numbers rising year on year according to UK Finance, from 154,614 in 2020 to 232,429 in 2023 a jump of 50%. While this rise was tempered with a slight dip in cases in the first half of 2024, the fraudsters are winning, getting away with more crimes, against more victims, year on year.

This picture is depressing; more people are falling victim to fraud each year, not less. However it has to be acknowledged that it is something that our banks and PSPs have limited control over. As explored above, fraud starts online and over the phone, well before banks and other PSPs get involved. Other than educating their customers about what to look out for in scams, the reality is that there is little a PSP can do to stop an APP fraud until a customer attempts to make the first payment.

Even when the instruction comes through from the customer to make what will later turn out to be a fraudulent payment, it would be unreasonable to expect every single one to be recognised immediately. Where antifraud measures should kick in is in catching the multiple payments, the patterns of behaviour that are typical of fraudulent activity.

The number of payments that are made per case, offers an excellent measure of the success banks are having in stopping fraud. While the figure is not provided by either the PSR or UK Finance it is possible to calculate from the data provided. According to UK Finance numbers there were 154,000 cases generating 245,000 payments in 2020, a rate of 1.6 payments per case. By 2023, despite the billions spent by the industry on tackling fraud, those numbers had gone up, to 232,000 cases and 417,000 payments, equating to payments per case of 1.8.

This metric, a 16% rise in payments per case, strongly suggests that banks are not having more success in stopping APP fraud. They are having less. Frauds are going on for longer, with more payments flowing from victim to criminal. The data is unforgiving. Across pretty much every type of fraud measured by UK Finance, be it investment, romance or impersonation, the number of payments made per case is up over the last four years.

Most strikingly, and worryingly given the pernicious nature of the crime, the number of payments made per case of romance fraud has nearly doubled over the last four years. In 2020 victims were making an average of 5.5 payments per case. Over the first half of 2024 that figure had leapt to 10.8. Here more than anywhere else we can see the urgent need for PSPs to act faster to stamp out fraud. The rise in the number of payments almost certainly equates to an increase in the length of time that someone is under the control of the fraudster, deepening the emotional and psychological harm that such crime brings with it, as well as the financial loss.

The problems banks are still having in correctly identifying and stamping out fraud were brought home in a case study presented to the APPG by the chief executive of an SME that suffered a prolonged, high value fraud[10]. While this was not an APP fraud the case does demonstrate how matters can get out of hand when a bank's anti-fraud measures fail.

> *Over a 15-month period Barclays allowed 118 transfers totalling nearly half a million pounds to be made from the accounts of one of its corporate clients to that of an employee of that company. The nature of the fraud was very simple, the employee, working in the payments department of the company that suffered the loss, simply substituted her own bank account details for those of a legitimate payee. Payments were made, despite Barclays flagging them as a mismatch.*
>
> *The problem though, was that Barclays processes only required it to check the payment anomalies with the person submitting the payment details - in this case the beneficiary of the fraud. No account signatory or other party at the client company was made aware of the repeated mismatch between the payee details and, therefore, the potential for fraud. In effect Barclays did little more than check whether there had been an administrative error, otherwise ignoring what should have been clear indicators of fraud.*
>
> *The matter only came to light when investigations carried out by the company revealed the losses. The potential crime was promptly reported to both the police and Barclays. While the police took the matter seriously and started a criminal investigation, Barclays refused to compensate their customer after carrying out what appeared to be a relatively limited investigation. Worse perhaps, when the customer continued to investigate what had gone wrong and whether it was down to deficiencies in the bank's systems, Barclays threatened to debank the customer by closing their accounts.*

The evidence provided by this kind of case study, while anecdotal, strongly suggests there is a lot more banks can do to crack down on fraud once it has started. By coincidence, the chief executive of the company that suffered the loss had a background in fraud prevention in the financial sector. He complained to the bank, explaining the weaknesses in its systems, how they could be addressed and asking for compensation. The complaint, and his criticism of the bank's processes, was rejected.

The scale of the problem is clear. Consumers are consistently exposed to scams, many of which are successful in convincing people to part with their hard-earned money. The gravity of the situation requires a regulatory response which both protects consumers when fraud occurs, and does everything possible to incentivise banks to prevent fraud from taking place in the first place.

In the UK, progress is being made. In response to the growing 'scamdemic', the UK government published a Fraud Strategy in 2023. A key part of this focusses on consumer protection in the form of a new regulation from the Payment Services Regulator which requires banks to reimburse the victims of fraud.

On compensation

It is now accepted practice that banks should compensate customers who have unwittingly fallen victim to fraud. While the APPG has no issue with this status quo, it is worth acknowledging how, viewed from a distance, this situation can appear curious. Why should banks pay for losses caused by third party criminality when they are doing no more than fulfilling client requests to transfer funds? This is particularly the case when you consider that the overriding legal, contractual duty on a bank is to follow customer instructions and complete transaction requests.

The reality is that as gatekeepers to the financial system banks and PSPs are uniquely placed to defend customers against financial crime. As such they have to act. This role and the responsibility it carries has grown over the last 50 years, with the creation of the Financial Action Taskforce in the 1980s, the Basel Committee of Banking Supervision in the 1990s and then the Wolfsberg Principles in the 2000s. These international agreements and the national regulations they have spawned have given banks statutory responsibilities to tackle financial crime.

Has the reimbursement limit been set at the right level?

In the UK this broad responsibility for dealing with financial crime led to the introduction of the PSR Mandatory Reimbursement Requirement (MRR) in October 2024. In its own way it was one of the most contentious regulatory interventions in recent memory. Not so much for what it did, but for what it didn't do. In its original form the scheme would have obliged banks to offer automatic compensation to customers who had fallen victim to fraud, up to a limit of £415,000. Concerted lobbying by the PSP industry[11], backed with support from politicians on both sides of the aisle, led to the cap being reduced to £85,000.

The main argument put forward by the banking industry to reduce the cap was that the higher limit put too much responsibility on banks and none on social media companies and other players who have a role in facilitating scams. They also argued that a higher compensation limit would act as an incentive for scammers to submit fraudulent claims for compensation as well as acting as a disincentive to consumers to act with care when making payments.

Some of these arguments clearly carry weight. As we explain above it should not be left to the financial sector alone to bear the cost of reimbursing customers. Social media companies should play their part. Some of the other arguments put forward for the lower compensation limit aren't as compelling. It is not clear that a higher limit on compensation would provoke a wave of fraudulent compensation claims. Banks are highly sophisticated at spotting fraud and should be able to identify and neuter fraudulent compensation claims at source. If banks can't protect themselves from fraud what chance do their customers have?

Equally, it is not easy to see how lowering the compensation limit will prompt customers to act with more caution when authorising high value payments. As explained in the PSR consultation, the mechanism to promote customer caution is not the upper limit on compensation, but through the claims excess, currently set at £100. Applying an excess to any kind of compensation, insurance or otherwise, is a recognised tool in shifting an appropriate level of risk back to the customer. It was introduced into the MRR precisely for this purpose and therefore should be the primary tool to engage customer responsibility. Once again, we believe more work should be done here to establish the drivers that could, and should, be used to affect customer behaviour. We will return to this in subsequent reports.

It is also highly debatable whether customers making higher value payments, in excess of £85,000, are really the ones who are acting carelessly. Research suggests such people are not the super-rich flinging money about carelessly, but individuals who are most exposed to financial risk, going through a once in a lifetime financial transaction, cashing in a pension or selling their house. Arguably these people need more protection than those who stand to lose lesser amounts of money.

Much more likely, and not entirely unreasonably, the battle to reduce the Upper limited was likely to have been driven by the potential cost to PSPs of compensating to the higher limit. According to the PSR[12] just 0.2% of cases fall into the £85,000 to £410,000 bracket. While this number is minuscule by volume, it is highly significant by value, accounting for around 20% of the total value of APP fraud. We estimate this percentage could be as much as £600m based on the APPG figure of £3bn for the total value of APP fraud.

It should be acknowledged that the change in compensation limit from £415,000 to £85,000 represents a significant transfer of risk from PSPs to their customers, a risk that PSPs may be better placed to understand, mitigate and manage than their customers are. The MRR is due to be reviewed over the current year. It is essential that data is gathered on the number and value of claims that fall in between this range during the last year in order to assess whether the cap on compensation has been correctly set, and whether any changes should be made to appropriately balance risk between banks and customers.

Perhaps more important than the upper limit, is the implementation of the scheme. On paper PSPs are required to act in a uniform manner, compensating all eligible customers and doing so within five working days. This was a significant driver in the implementation of the new regulations, levelling up a playing field that was significantly out of kilter under the old Contingent Reimbursement Model (CRM).

The CRM was deficient on two basic levels, firstly it was voluntary; secondly it produced wildly different outcomes. To give a snapshot, in 2023 Nationwide refunded 96% of scam cases in full, according to PSR data. The Co-operative Bank, another signatory to the scheme, had a reimbursement rate of just 55%, albeit with a further 16% refunded in part. Unsurprisingly firms outside the scheme were much, much worse. Monzo refunded just 9% of cases and AIB just 3%. These yawning disparities are not just unfair on customers, they also introduce

competition issues between firms and raise questions about the approach of the firms that are failing to pay compensation. While it is by no means exact, there appears to be a broad correlation linking firms that fail to pay compensation with those firms that are subject to a higher volume of successful scam attacks.

Reimbursement data from the PSRs is very useful but does not provide the full picture. If we want to really understand how banks are dealing with the thorny problems of reimbursement we also need to see what channel reimbursements are flowing through and how fast they are processing claims. This would mean breaking out the value and volume of payments that are being made directly to clients within the five-day target against payments that are being made after intermediation by legal representatives or through the Financial Ombudsman Service (FOS). The PSR and the FOS need to work together to establish how these data points can be extracted and presented so they are timely and publicly available.

This data should be provided both contemporaneously and historically. Monitoring the relative change in the number of cases going through FOS will be key to understanding the success, or not, of the PSR reimbursement scheme. This is particularly the case where early evidence suggests different banks are taking very different approaches to dealing with claims. While some are processing them in line with the spirit and letter of the PSR guidance, others are taking a far more adversarial approach, declining claims for what feel like premeditated or spurious reasons. We talked at length with Richardson Hartley Law, the law firm sponsoring this report, about their experience of how banks are dealing with the compensation claims. The response was worrying. One of their senior solicitors explained:

> *We are receiving responses from the banks which demonstrate that they are not reading the Letters of Complaint being submitted on behalf of clients and instead appear to be adopting a policy-based approach of rejecting legitimate claims from the outset. For example, we have just received a response from Santander which rejected the complaint on the basis that the client had authorised the transfer of the funds to an account with another bank in the client's name. This was incorrect as the funds were in fact transferred to the fraudster's account which was in the fraudster's name with a different bank. How can you explain this glaring error by the bank other than by concluding the bank simply didn't read what we had written in our letter?*

Another solicitor from the same firm reported:

> *We are experiencing a number of hurdles from the banks when attempting to contact them by telephone in terms of them not accepting signed Letters of Authority and stipulating that the client needs to be on the call with us or refusing to connect us to the relevant department dealing with the complaint. In one instance Revolut incorrectly advised that we needed to have a Power of Attorney in order for them to discuss the client's account with us. This is simply wrong, in law and in practice.*

The reflections above are no more than straws in the wind. To really know what is going on and whether banks are acting in accordance with the PSR guidance we need more data. This extends to the Financial Ombudsman Service. Analysis of complaints registered with the FOS suggests that the number relating to APP fraud and wider scams has rocketed in recent years. Searching the database for complaints that respond to the terms 'scam' or 'authorised push payment' shows the number of complaints going through FOS tripling over the last three years.

The measure, searching for keywords across the FOS database, is inexact and will result in false positives, however it does provide an indication of the volume of cases and their direction of travel. It also allows us to get a snapshot of how different banks are dealing with cases and the wildly divergent outcomes that would appear to flow from different banks. Analysis of data across 2023 shows there were just under 700 cases where the decision report responded to the search term 'authorised push payment' fraud. Of these 9.5% are complaints against Lloyds Bank, 9.1% are against Barclays and just over 1% are against Nationwide. Given the position these three banks hold in the market these are fair, even encouraging returns, suggesting the banks are not pushing an outsized proportion of complaints to FOS. The tiny return for Nationwide no doubt reflects the firm's straightforward approach to refunding against scams, as detailed above.

Cast a glance at some of the challenger banks and the position is very different. Given its size Monzo is by far the most complained about bank clocking 13% of all decisions. The proportion of those decisions that go against the bank is also well out of line with the rest of the market, 63% of complaints being upheld by FOS, against an industry norm of about 30%. The figures relating to Revolut are no less startling, the number of complaints ending up at FOS out of

proportion to the size of the firm and being upheld in numbers that are much higher than the industry standard. This kind of information, suggesting a failure by certain firms to properly address their responsibilities, requires investigation and response from the PSR.

Equally, the speed at which banks and PSPs are responding to compensation claims appears to be a long way from the spirit and letter of the CRM. Anecdotal evidence suggest that some firms are either not responding to fraud reports and compensation requests, or taking far, far longer than the five days now mandated by the MRR. The inexplicable and, in some cases inexcusable, differences in approach between different banks were clearly demonstrated in the case of Mark Beer.

> *Mark Beer thought he had done everything right. Before paying £9,500 to buy a motorhome he had gone into his bank, Santander, with the correspondence around the purchase to check it was all ok. "I went into Santander before I made the payment because I wasn't sure about it," he explained. "I showed them all the correspondence I had, including the emails from the 'PayPal personal helper'. The woman behind the counter said it was a valid bank account and it should be fine - those were her exact words."*
>
> *Mark made the payment there and then, on 15 August 2023, into an HSBC bank account, with the motorhome due to be delivered a week later. When it didn't arrive, he contacted the delivery company. "They didn't know anything about it, and so I knew instantly that it was a blag," he said. "It was very upsetting. And the van was back up for sale with a different number plate a few days later."*
>
> *Santander initially tried to blame Mark for transferring the money, but eventually agreed to pay him half of the £9,500, with the other half to come from HSBC, the receiving bank. But more than a year later, HSBC has still not paid up, and Mark has had to enlist a specialist firm of fraud solicitors to recover the rest of his cash.*

Consistency begins with the regulators – the need for greater alignment

The disparity in how firms deal with compensation claims is a serious concern and spills over into other areas where customers risk being unfairly exposed to risk. Under the current MRR firms can reject compensation claims for reasons that are questionable at best. One key area is around fraud warnings, which we cover below. Another reason for rejection centres on how payments are made.

Under the current rules if fraudulent payments are made by a customer to another account in their name (me-to-me payments), to a cryptocurrency account or overseas, a bank can reject compensation. While there may be superficial reasons why this makes sense, the practical reality is it is illogical and counterproductive. All three of these payment types can be indicators of fraud. What fraudsters will do, typically, is ask their victims to first make payments from their

established bank to a challenger bank and from there into a cryptocurrency account overseas. To carve these payment types out of the compensation system is akin to inviting firms not to police these types of transfers and to undermine customer confidence in these transactions.

This problem has been recognised by the Financial Ombudsman Service who have found that compensation claims exhibiting these characteristics should be paid out by firms. If that is the case, why should they be rejected under the MRR? To do so does no more than prolong a compensation claim, turning a one stage process into two, and saddling the FOS with more claims and more work.

There needs to be much more alignment between the FOS and the MRR. Another area where they currently do not match is around the timescales for compensation. Under the MRR banks have a five day deadline to compensate customers. We have no data on performance to this target, however the overwhelming anecdotal evidence is that they are not hitting this target in many cases. What then should customers do? FOS do not accept cases after just five days, instead working to an eight-week period after the complaint has been made. Either this or the FOS requires that cases have been rejected by the firm before they will take them on. But what if the complaint is that the firm is not dealing with the matter, how can that issue be resolved? It's an uncomfortable situation, and which requires the regulator to investigate and enforce.

On this final point, action taken by the regulator to enforce compliance with the MRR, there is clearly a case for far more input by the PSR or FCA in the future. The regulator should require firms to be updating it in real time about compliance with the scheme, this would include timescales, rejection rates and details about the complaints and how they were paid out. The MRR is due to be reviewed at the end of the first year. At the moment we are all in the dark as to how it is operating. Only a closed circle of insiders really know if it is functioning well. This cannot continue and therefore we are calling for increased and improved transparency and data, as outlined in our recommendations section below.

A regulation is only as good as its enforcement

The PSR has enforcement powers, both to gather information and to impose financial penalties where compliance failures are identified. In the 10 years since the regulator was created it has published only four enforcement notices, three of which resulted in fines. This lack of action is only compounded with respect to the management of the MRR, given the implementation of the scheme is not being managed by the PSR, but has been outsourced to pay.uk, an industry body set up the banking industry. This obvious conflict of interest was identified by the Treasury Committee in its 2023 report into APP fraud, 'Scam reimbursement: pushing for a better solution'[13]. The Committee recommended that the PSR be more directly involved in the management of the MRR scheme. Despite this nothing appears to be done and pay.uk took on a role it appears unsuited to manage. As recommended by the Committee, this structure needs to be assessed as part of the one-year review into the MRR.

Fraud warnings – the regulation is designed not only to protect, but to incentivise prevention

A separate, but equally significant concern for the APPG is the approach to fraud warnings taken by the banking industry. Warnings, alerting customers to the risk of fraud, are now ubiquitous. Anecdotally, it would appear that banks are publishing fraud warnings every time a customer makes an online instruction to transfer money. More than this, some banks are publishing fraud warnings, not as a payment is being made, but as a customer signs in to their account. Pages, such as one we saw from Santander, ask customers if they want to know how to "spot a fake deal" with the option of pressing two buttons, one being "protect yourself" the other "not interested". While this kind of customers engagement may be done with the very best of intentions the concern is it could also be used against the customer.

Equally for the customer it would be all too easy to think that they did not qualify for any reimbursement because of the volume of fraud warnings they have received. The reality is customers are not ignoring fraud warnings because they don't care about fraud, rather it

is down to coping with everyday pressures. People don't have time for fraud tutorials every time they go online to check their bank balance. This type of quite normal behaviour should not be used by banks as a reason to refuse compensation.

In various consultations on its compensation scheme, the PSR made it clear that while customers should be required to have regard to warnings, such warnings should be "… consumer, scam and transaction-specific."[14] The regulator went on to state that warnings should not be boilerplate messages and that firms "…would not be able to legitimately refuse reimbursement claims based on vague, non-specific warnings or warnings that routinely accompany most or all transactions of a similar type."

While this is a sensible approach, the truth is, it does not go far enough. The reality is that we are all getting carpet bombed with 'vague, non-specific or routine warnings' at present. The danger is that they are so commonplace as to become a background noise. It is quite possible that most of us already ignore these messages, most of the time. It is crucial that the regulator monitors how fraud warnings are being used, their frequency and content to ensure they are effective in deterring fraud and not being used as a reason to turn down compensation requests.

In summary, if the new PSR compensation scheme is to work it will need to satisfy various criteria. It will need to protect customers from fraudsters, incentivise the banks and PSPs to build effective defences against fraudsters and help create the conditions to stamp out fraud. In an ideal world it would be a short-term fix to a temporary problem. At present we have limited data on the performance of the scheme, something that should be addressed ahead of the one-year review.

Conclusion

While there is much more that can be done to tackle APP fraud, we should first acknowledge that significant steps have already been taken. The Government, the regulators and the finance industry are as one in agreeing this is not something that can be ignored. This consensus has led to huge investment by banks in anti-fraud measures, legislation by Government to tackle the problem and the creation of the MRR by the regulator.

At the same time even the most optimistic commentator could not claim that the problem is under control. Case numbers remain high while the total value lost to APP fraud each year is far higher than previously thought, £3bn by our estimate. Against this backdrop we must do more to disrupt the business model that underpins fraud, while also protecting customers and the wider financial system. We are still at the very early stages of understanding how the new compensation scheme and improved fraud prevention measures are working. The APPG will have further recommendations later this year in our follow-up work to this report. However this should not mean we can't already act to improve on the process. With this in mind, the APPG has the following recommendations:

- All PSPs to be required to establish a clear pathway for reporting fraud across all platforms, websites, apps, call centres and in person. Customers will have their own preferred method of communicating with their banks, which needs to accommodate in fraud reporting. One-size does not fit all. If banks do not provide a clear pathway for fraud reporting it may be necessary to look at creating a centralized system where frauds can be reported, data collected and performance monitored.
- Greater disclosure of APP fraud numbers and types. This should include disclosure of the following data points:
- Average number of payments per case, broken down into specific fraud types
- Numbers of complaints relating to non-payment of compensation for APP fraud losses that end up with FOS. Data to be sub-divided by firm.
- Compliance with five-day target for compensation under the MRR scheme.
- Social media companies to be required to contribute towards the MRR and the Economic Crime Levy. The Government to legislate, or act on existing legislation, so that social media companies are held accountable for their success, or failure, in tackling fraud.
- PSR to monitor how fraud warnings are being used, their frequency and content to ensure they are effective in deterring fraud and not being used as a reason to turn down compensation requests.

Methodology

This report has drawn heavily on the work of the banking industry, the Payment Services Regulator and other third parties, such as our sponsor Richardson Hartley Law, who have dug into their files to provide us with the bulk of the case studies reproduced above. The data points we have accessed are detailed in the report, however we should give credit to UK Finance and the PSR for their annual / bi-annual reports on fraud and the wealth of data they contain. Both reports contain fascinating and detailed insight into the extent of the problem.

We sent questionnaires to all the main banking groups, UK Finance and the PSR giving them an opportunity to provide their views on the problem and its solution. The bulk of the PSPs we contacted took the not unreasonable view that it was more efficient to allow UK Finance to comment on their behalf. Both UK Finance and the PSR provided us with very detailed and comprehensive feedback.

Endnotes

1 While not strictly the same, this report has used the terms 'banks', 'firms' and 'Payment Service Providers' or 'PSPs' as synonyms throughout this report.

2 https://committees.parliament.uk/committee/102/justice-committee/news/173618/justice-response-inadequate-to-meet-scale-of-fraud-epidemic/#:~:text=The Committee finds that the,for 40% of reported crime.

3 During the drafting of this report the Government announced it was to subsume the PSR within the FCA. As this was not due to happen until sometime after this report had been published this change had not been reflected in the body of the report.

4 https://www.cifas.org.uk/newsroom/stateofscams

5 Carter, E (2021). Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud.

6 This case study was originally published in The Times. Like many of the case studies in this report it was sourced from cases handled by the sponsor of the report, Richardson Hartley Law.

7 https://www.psr.org.uk/information-for-consumers/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age/

8 https://about.fb.com/news/2024/10/meta-partners-with-uk-banks-to-combat-scams/

9 https://www.ukfinance.org.uk/system/files/2024-06/UK Finance Annual Fraud report 2024.pdf

10 This case study has been anonymised as there is a risk it could become sub judice due to the ongoing police investigation

11 Data released as part of a Freedom of Information request showed that between 19/12/23 and 04/09/24 (the dates when the higher and then lower compensation limits were announced) senior executives at the PSR had 93 meetings with PSPs. While this appears to be a high number the PSR was not able to provide data for previous years by way of a comparator.

12 p16 of PSR consultation paper: https://www.psr.org.uk/media/jplkxij4/cp23-6-app-fraud-excess-max-cap-consultation-paper-aug-2023.pdf

13 https://committees.parliament.uk/publications/33811/documents/184643/default/

14 https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf

appg Fair Banking