The psychology of scams
Understanding why consumers fall for APP scams
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About</td>
<td>3</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>3</td>
</tr>
<tr>
<td>Executive summary</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Methodology</td>
<td>8</td>
</tr>
<tr>
<td>Report structure</td>
<td>9</td>
</tr>
<tr>
<td>1. The opportunity</td>
<td>10</td>
</tr>
<tr>
<td>The impact of Covid-19</td>
<td>12</td>
</tr>
<tr>
<td>The importance of context</td>
<td>13</td>
</tr>
<tr>
<td>2. The scam</td>
<td>15</td>
</tr>
<tr>
<td>Imitation</td>
<td>16</td>
</tr>
<tr>
<td>Building relationships</td>
<td>18</td>
</tr>
<tr>
<td>3. The payment</td>
<td>21</td>
</tr>
<tr>
<td>Creating urgency</td>
<td>21</td>
</tr>
<tr>
<td>Scammers coach and manipulate a victim through the payment</td>
<td>24</td>
</tr>
<tr>
<td>Warnings at the point of payment won't always stop the scam</td>
<td>25</td>
</tr>
<tr>
<td>4. The aftermath</td>
<td>27</td>
</tr>
<tr>
<td>Realising you have been scammed is highly distressing</td>
<td>27</td>
</tr>
<tr>
<td>Dealing with the bank and other institutions can add further distress</td>
<td>28</td>
</tr>
<tr>
<td>Decisions and actions by banks and others are not being explained clearly enough</td>
<td>30</td>
</tr>
<tr>
<td>5. Recommendations</td>
<td>32</td>
</tr>
<tr>
<td>A fairer system of redress</td>
<td>32</td>
</tr>
<tr>
<td>More effective support for banking customers</td>
<td>34</td>
</tr>
<tr>
<td>Tackling wider weaknesses</td>
<td>36</td>
</tr>
</tbody>
</table>
About

Which? is the UK’s consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We’re the independent consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we’re not for profit and all for making consumers more powerful.

Basis is an independent strategic insight consultancy that fuses a range of approaches – including quantitative and qualitative primary research, behavioural sciences, cultural insights and semiotics – to unlock opportunities for brands and organisations across the globe. Their work has been recognised as best-in-class at the prestigious Market Research Society awards in 2019, 2020, 2021 and 2022.

Acknowledgements

Which? would like to thank the team at Basis for their excellent research, analysis, work and support. The views and opinions expressed in this research are solely that of Which?.
Executive summary

Too many consumers are being let down by the voluntary authorised push payment (APP) scam reimbursement scheme. Currently, there is a lack of systematic oversight of the way the scheme is implemented. The banking industry has a financial incentive to act stringently with the reimbursement of victims but the industry is also, in effect, both judge and jury. Poor rates of reimbursement for victims suggests implicitly that victims themselves are often to blame for the scam. We must ensure new regulations do a better job of giving justice to victims.

Our new research draws on 20 in-depth interviews with APP scam victims. Our aim was to understand their scam journeys and draw out common factors and themes which led to them being scammed. We found:

• Scams often occurred when the victims were beyond their emotional ‘window of tolerance’ i.e. they were especially stressed, tired or distracted. This meant victims were more susceptible to being defrauded and often not able to perform the same level of checks they otherwise would have.

• Common psychological biases made it difficult for people to detect the scams once they began engaging with the scammer. Scammers built relationships with their victims or imitated trusted people or institutions in order to manipulate their victims in ways that reduced their ability to question what they were being told. The tactics also successfully trigger unconscious biases in human decision making, in particular: authority bias, liking bias and similarity bias, which impairs our ability to make logical decisions.

• We identified two primary tactics scammers use to push their victims to make payments: creating an overwhelming sense of urgency and coaching and manipulating the victim past their bank’s warnings and other potential points of intervention.

• Once victims believed the scammer’s story and persona, they found it very difficult to detect fraud and so were not able to defend themselves against the crime. This is not to say that our research participants didn’t try to protect themselves; often they questioned the scammer, or tried to undertake checks, but the manipulative behaviour of the fraudster meant this wasn’t sufficient to lift the spell of the scam.

This research helps us understand what scam victims are up against and the extent to which individuals can protect themselves from scams. In doing so, it both makes a case for fairer reimbursement practices, and for better action to prevent scams, helping to keep consumers safe.
We recommend urgent action in three key areas:

1. A fairer system of redress
   • The Payment Systems Regulator (PSR) should proceed with its proposals for a reimbursement obligation for all payment service providers that:
     – Applies in all but exceptional circumstances
     – Fully protects victims who were especially vulnerable
     – Covers all types of APP scams
   • The Government should legislate so that scam victims can take action to enforce their rights directly against firms that are in breach of these obligations.
   • The PSR should provide regulatory oversight of the new reimbursement obligation and take enforcement action against firms that do not meet its expectations.
   • The PSR should require all payment service providers to report and publish data on APP scam levels and reimbursement.
   • The Government should carry out a broader review of consumer protections for different payment methods.

2. More effective support for banking customers
   • All payment service providers should train relevant staff on how to support victims of APP fraud.
   • All payment service providers should be required by the PSR to share standardised data with each other on fraud risks before making a transaction.
   • Payment providers should continually test and improve the effectiveness of their customer fraud warnings and consider other risk-based interventions.

3. Tackling wider weaknesses
   • Ofcom should ensure that all telecommunication providers offer the same protections to consumers to prevent number spoofing.
   • The Government should pass an improved Online Safety Bill into law to prevent users from encountering fraudulent content online.
   • The Government must do more to help facilitate effective data sharing and reporting systems across industry and regulators to tackle fraud, and empower consumers to report scams.
The UK is in the midst of a fraud epidemic. Reported payment fraud hit £1.3 billion in 2021.\(^1\) £583 million of this was via authorised push payment (APP) scams, where victims are tricked into sending money to a fraudster.\(^2\) Losses have risen year on year since Which? issued a super-complaint in 2016, highlighting the lack of protection for victims compared to other types of fraud.\(^3\)

Behind these financial tallies are the victims of crime. Beyond financial losses, being a scam victim is associated with lower levels of happiness and life satisfaction, and greater anxiety. Which? estimate the harm from lost wellbeing attributable to scams amounts to £9.3 billion a year.\(^4\)

Consumers are put in harm’s way by a myriad of weaknesses in everyday systems – social media platforms hosting fraudulent adverts, online marketplaces selling fake goods, telecoms companies allowing scammers to spoof numbers and banks allowing fraudsters to operate accounts. Despite these wider enablers of fraud, consumers are all too often left to themselves to avoid becoming a victim or to shoulder financial losses.

A system-wide approach is needed to stop the source of scams. Individuals also need to play their part to prevent and report suspected fraud. But this needs to be rooted in an understanding of human behaviour, rather than victim-blaming. We must acknowledge that the wrongdoing is on the part of the fraudster, and that people do not set out to be scammed.

Two major pieces of legislation currently going through parliament rightly seek to put greater responsibility on key industries. The Online Safety Bill will place duties on online platforms including search engines, social media and dating apps, to have processes designed to prevent or minimise the risk of users encountering fraudulent user generated content and fraudulent advertisements. The Financial Services and Markets Bill will help establish an obligation for banks and other payment providers to reimburse victims of APP fraud. Which? has long campaigned for both of these reforms, and they cannot come soon enough.

Which?’s recent report in collaboration with Demos Consulting analysed the character of potentially misleading and fraudulent investment adverts on Meta platforms, Facebook and Instagram. The report calls for more comprehensive action and a holistic approach to tackle online scam adverts. As well as making the case for The Online Safety Bill, it also calls for the Government to bring forward further legislation to tackle misleading and fraudulent adverts across the rest of the web through the Online Advertising Programme, and for joint action by platforms and other stakeholders to share data and insight to stop scammers reaching consumers.\(^5\)

---

5. Which?/Demos Consulting (2022), *Capital at risk: How platforms can do more to tackle misleading and fraudulent adverts online*
The main focus of this report is on reimbursement for victims. Some argue that it is unfair to hold banks totally liable for APP scams given the role of other industries in enabling fraud, and that we should instead wait to design a system that includes financial contributions from a wider range of related industries. We agree that other industries, such as social media platforms and search engines, should be given legal responsibility for preventing fraudulent content with tough enforcement powers for regulators including fines. However, we have yet to see a credible proposal as to how failings within these industries could be tied directly to an individual scam case for the allocation of liability for reimbursement. Six years on from our super-complaint on this issue, we cannot wait any longer to address the glaring gap in consumer protection for authorised bank transfers.

The payment may be the last step in the scam, but the choice of payment method and the payment provider is not an afterthought for fraudsters but integral to the scam. Fraudsters have to plan ahead with how they will receive and launder these funds, either operating an account directly or via money mules. Most scams involve a payment between two UK accounts first, to help avoid suspicions, so fraudsters typically target the weakest points in the UK’s payment systems. It is no accident that the prime target is currently the Faster Payments scheme, where there is no explicit requirement for banks to reimburse victims when a payment turns out to be to a fraudster, unlike for many other payment methods such as cards. As we have long argued, this lack of consumer protection means there are insufficient incentives for banks and other payment providers to prevent authorised fraud. Addressing this gap in consumer protections is therefore as crucial to our attempts to prevent fraud as it is to providing a fairer system of allocating losses.

Putting a reimbursement obligation on the payment firms involved in a fraudulent transaction is by no means novel. For unauthorised bank payment transactions, this has been a clear statutory requirement for UK transactions since 2009 with the exception of cases where victims are ‘grossly negligent’. The principle that victims should be reimbursed by the banks involved in the payment has already been established by an industry reimbursement code for authorised push payment scams introduced in 2019. 10 of the largest banks have signed up to this Code, covering 90% of transactions. However, this Code has failed to provide fair and consistent outcomes for victims. Around three in four cases that have been reviewed by the Financial Ombudsman Service since 2019 – a process that further adds to the emotional and financial strains on victims – have sided with the victim, highlighting the lottery of outcomes that victims still face.6 Our own work has highlighted issues with the four overlapping and inconsistent exclusions for reimbursement that banks can choose from in the Code, and the lack of appropriate regulatory oversight and enforcement to hold firms to these standards.7

The Payment Systems Regulator has proposed a simpler and fairer reimbursement obligation that would apply to approximately 400 payment service providers. It would bring protections into line with those in place for unauthorised transactions. Some stakeholders have argued that this could lead to ‘moral hazard’, with consumers being knowingly reckless when making payments because they are aware that they are more likely to get their money back if things go wrong. However, we are

---


7 See, for example: Which? (2020), Reimbursement for authorised push payment fraud Consumer experiences of the Contingent Reimbursement Model Code, available here https://www.which.co.uk/policy/money/6249/pushpaymentfraud
not aware of convincing evidence to suggest that customers take less care when making payments due to an awareness of consumer protections. There is already a real-life experiment that suggests this theory is unfounded. TSB launched a higher level of protection for its customers under its Fraud Refund Guarantee in 2019, which has led to reimbursement in 98% of all fraud cases including unauthorised and authorised transactions. TSB has been clear that it has not seen evidence of additional moral hazard or any significant change in the amount of fraud being reported as a result.

For mandatory reimbursement to work, firms must base their decisions on the reality of victims’ experiences rather than assumptions and beliefs. Our aim is to show what expectations we can have for human behaviour for someone being tricked, lied to and manipulated within a scam. While case studies of scam victims are often published in the media, our research goes further by analysing and understanding the scam journey stage-by-stage in detail. Recognised psychological frameworks are used to help build understanding of scam victims perceptions’ of the scammer, and to explore their decision-making and behaviours. Through interviews with twenty victims of APP fraud, we drew out the common tactics and tools used by scammers to manipulate their victims.

**Methodology**

Which? commissioned the independent research agency Basis to conduct qualitative interviews with 20 victims of Authorised Push Payment fraud across July–August 2022.

Basis researchers spoke with two Which? experts on APP fraud. One works within Which? Helplines, and has extensive experience of supporting APP fraud victims. The second is a Which? journalist specialising in financial affairs including APP fraud. Basis also spoke to an independent clinical psychologist to understand the theories that help explain the psychology behind victims’ experiences.

To recruit victims to partake in the research, Basis approached an independent recruitment agency which maintains a pool of potential research participants. The participants were then recruited to ensure an even mix of scam types, with five interviewees from each broad scam type: impersonation, investment, purchase, romance. Participants were also recruited to ensure:

- A mix of ages, genders, socio-economic group, and household status.
- A mix of those reimbursed and not reimbursed.
- All respondents could sufficiently remember in detail what happened during the scam (17 of 20 victims were scammed in the last 18 months. Those that were not were asked to verify they could remember the experience in detail.)
- A mix of financial losses (a minimum threshold of £500 was set.)
- All monies lost were through bank to bank transfers.

Victims had an initial 30 minute video-call with researchers to establish rapport and ensure victims were willing to share their story in the level of detail required for the research. 90 minute semi-structured interviews were then conducted in which respondents described their experience of being scammed in detail with trained researchers. Five interviews were held in person and 15 via video-call.

---

8 [https://www.tsb.co.uk/fraud-prevention-centre/fraud-refund-guarantee/](https://www.tsb.co.uk/fraud-prevention-centre/fraud-refund-guarantee/)
Interviews were semi-structured, using a guide of questions and tools to understand the victims’ journey with follow up probes tailored to individual victims. Tools included: an ‘emotions wheel’ to help participants to name their feelings at different stages in the journey and psycho-drawing exercises to further help participants express their relationship with, and perceptions of, the fraudster during the scam.

Basis analysed the results to identify common themes across victims’ journeys, including similarities in the tactics used by APP scammers. Psychological frameworks such as the Window of Tolerance, Wise Mind Model, unconscious biases, and Cognitive Dissonance were used to ground the findings in established psychological theory. The results of these were presented to Which? in a final debrief. The presentation and redacted transcripts were then shared with Which?. Transcripts and the final debrief were both further analysed by Which? researchers and used to create this report.

The stories presented here are case studies from these interviews and excerpts from transcripts. The names and other details have been changed where necessary to protect participants’ anonymity.

Report structure
This report details the experiences of the twenty scam victims we spoke to on a stage-by-stage basis.

**Chapter 1: the opportunity.** This chapter aims to understand the life context of the victims we spoke to, when they were contacted by their scammers, and how this affected their susceptibility to being scammed. We outline how the victims were commonly feeling at the time of the scam and base this in psychological theory.

**Chapter 2: the scam.** This chapter details the typical tactics of the scammers we heard of during the scam itself. We see how these scammers deceived their victims using imitation and relationship building in order to build trust and credibility in the minds of the victims. We see why these tactics work through the Wise Mind Model and through unconscious biases.

**Chapter 3: the payment.** Here we learn how scammers induced payment from victims within this research. We learn how the scammers created a sense of urgency in the victims and how scammers manipulate and coach and why these work, explained within psychological biases.

**Chapter 4: the aftermath.** In this chapter we see the immediate impact of the scam on the victims we spoke to and how their interactions with the bank and other institutions affected their long term thoughts and feelings about the scam.

**Chapter 5: recommendations.** We offer our recommendations for industry, government and the Payment Services Regulator as to how, when and why victims of APP scams should be reimbursed following a scam.
1. The opportunity

Often in life, unfortunate events feel like they are coming all at once. The car breaks down right before a holiday. Your daughter texts asking for money as you get back from looking after your elderly parents. The landlord of a new flat disappears after you’ve paid your deposit, right when your final exams are taking place.

Unfortunately for the scam victims we spoke to – this is precisely what happened. Many were experiencing periods of significant distraction, acute stress or serious emotional strain. They were preoccupied just as they were targeted by a fraudster.

The impact of moments of severe strain on our ability to think and reason clearly can be explained through the concept of the ‘window of tolerance’. This describes the range of tolerable emotional strain a person can deal with. Outside of your ‘window of tolerance’, decision making can be impaired.

**Windows of tolerance**

An individual’s ‘window of tolerance’ is their personal range of tolerable emotional stimulation. Inside this window a person is comfortable in their emotional state. They are able to self-regulate their feelings and therefore able to think clearly, act with consideration, and relate well to themselves and others.

However, a person may be pushed to the limit or outside of this window by stimulating environments, stress, worry or the accumulation of smaller pressures.

When outside their window a person is in a state of ‘hyper-arousal’. Hyper-arousal occurs if a person is dealing with too many emotional or stressful situations at once.

“In this situation, people don’t think; they feel something intensely and act impulsively.”

Under certain circumstances, an individuals’ window can become narrower, whereby they are then less able to tolerate more stressors and stay within that window, and more likely to be tipped into a state of hyperarousal.

“Being emotionally worn, physically exhausted, or surprised by an interaction can each narrow the window of tolerance. In such cases, an individual may become emotionally wrought up or visibly upset by an encounter that, under other conditions, would have occasioned only mild arousal.”

We found that many of the scam victims who participated in our research were at the limits or outside of their own window of tolerance. They were already stressed, worried or anxious. This was sometimes due to major life events such as a parent being very unwell, and in other cases was caused by the accumulated pressures of everyday life: being busy at work, studying for exams or moving home. When the victims we spoke to were pushed beyond the limits of what they could comfortably deal with, they were less able to spot the scam. They did not have the time or the mental space to reasonably cope with or question a new problem in the same way they might have done if the timing had been different. We see this very clearly with both Susan and Lyla below.

Susan, 64. Impersonation scam. Lost: £2,200. Fully reimbursed

Susan was messaged by an unknown number, a scammer, pretending to be Susan’s daughter. The message said she had dropped her phone down the toilet the day before, and so had a new phone but also had lost access to her online banking. The scammer then asked for £2,240 to help repay a loan which was “due yesterday”.

Susan’s first thought was:

“Oh, I don’t have time for this”

Susan’s dad was recently out of hospital (and would die two months later) and Susan was undertaking most of his care to reduce the burden on her mum, who had recently had a stroke. Susan’s sister was also staying, and had argued with Susan’s partner the night before, causing Susan and her partner to argue too.

“I was feeling quite stressed at the time. I did think ‘oh what is this for?’ [at her daughter’s message] but then thought ‘I really can’t delve into this right now’. My mind was elsewhere.”

Susan sent the money. Only when the scammer then asked for a further £3,100 did she realise she was being scammed and began to panic.

Lyla, 41. Impersonation scam. Lost: £3,000. Reimbursement denied.

During the pandemic, Lyla was working 12 hour shifts and her husband, a taxi driver, was out of work.

“It was a nightmare. I was working long hours to try to stay on top of our finances. I was frustrated and exhausted.”

Lyla received a message from her sister’s number about an investment opportunity. This was not unusual as she and her sister regularly spoke about finances together.

“She asked me a few times over the space of a week or two whether I was interested. I looked at the website and it all looked good and above board and promised quick returns. I kept meaning to call her to ask more about it but I was so busy with work that by the end of my shift I would forget all about it.”

Unfortunately, unbeknownst to Lyla, the messages were not from her sister but from a scammer who had hacked her number.

Lyla was sceptical but the scammer showed her screenshots of bank statements showing the money that ‘her sister’ had already been making from it.

“It was a lot of money. Five grand. Ten grand. I was worried about sending the money but also thought that this money could get us out of the hole we were in.”

Only after several weeks, when she eventually saw her sister in person and questioned her on the investment, did Lyla realise she had been scammed.

Both Susan and Lyla were stressed and emotionally exhausted before being contacted by the scammer.

Susan simply wanted to get back to caring for her dad, and ensure her mum was not overburdened. The compounding emotional strain of these responsibilities, along with managing a fractious relationship between her partner and her sister, meant Susan was nearing the edge of her window of tolerance. When her daughter then asked for help, she was too distracted to question the request.

Lyla’s working life was extremely busy and there were increasing money worries as her partner was unable to work. She was nearing the limit of her window of tolerance. So when her sister shared a chance to relieve some of those worries and make extra money, she didn’t question this as she otherwise might have done.
There were similar stories for others we spoke to too, all of whom were already nearing the edge of their window of tolerance prior to contact with the scammer:

---

**Christine, 26. Purchase scam. Lost: £1,000. Reimbursement denied**

Christine was completing her final law exams in a noisy house-share with a mother and newborn baby, and so was struggling to concentrate. Feeling her future was on the line, she found an affordable flat online and felt pressured by the landlord, who cited the oversubscribed London rental market, to send over a deposit before viewing. Feeling she needed to act quickly, Christine transferred the money. The landlord quickly disappeared.

---

**Oliver, 44. Impersonation scam. Lost: £600. Reimbursement pending**

Oliver was rushing to a work meeting when being told by ‘HMRC’ that he must settle an outstanding tax bill. He had seen and skimmed an email from HMRC several days before and was now being told he might face prison if he did not pay soon. Oliver was panicked and stressed about being late to his meeting and, in a rush to get them off the phone, he transferred the money.

---

**The impact of Covid-19**

The pandemic proved a fruitful time for scammers. UK Finance reported that the total volume of APP scam cases increased by 22% between 2019 and 2020 to 149,000 cases. Within this research we also saw how APP scammers took advantage of the turmoil, as shown by stories like Lyla’s. For many consumers, the sudden change in routines, lifestyles, and finances meant that people felt more desperate and were often too exhausted or distracted to be able to think through the situation as they might have otherwise done.

Lyla was feeling short of money as her partner could not work and she was working 12 hour shifts. She was exhausted, felt a greater need to make some money in another way and was reassured by what her sister had sent her.

For Katie, Covid meant she was detached from her friends and family. She felt lonely and sought companionship online.

---

**Katie, 52. Romance scam. Reimbursement denied.**

In November 2020, in the middle of the UK’s second lockdown, Katie was alone at home with her teenage son, who was usually upstairs in his room. Unable to visit her friends or family and so was looking for companionship.

“At the time, I was feeling isolated and lonely as well.”

A friend told her about a website for meeting new people. Despite having never done anything like this before, she signed up.

“My friend wasn’t dating on there, just making friends. I also made quite a few friends on there.”

She then met a man from the USA and started regularly speaking to him. After a couple of months of talking online she said their friendship had become an online relationship. The man soon asked for £200 to help with medical bills for his daughter, which he returned not long later – building trust in Katie’s mind. Soon after he asked for money totalling £4,000 for medical bills and for help with his business, which Katie also sent.

In January 2021, her brother found out about the relationship and being suspicious, messaged the man himself. The man then blocked Katie, and she knew she had been scammed.

---

However, the impacts of Covid-19 on the lives of ordinary people are not relics of time. Unfortunately, the current cost of living crisis will also place profound strain on people’s ability to work, to pay for things they want, and to socialise. The crisis will likely mean many seek alternate ways to make money as their standard of living declines. Many will be pushed towards or outside their window of tolerance, making them vulnerable to scammers. There is some existing evidence that scammers are already adapting their techniques to take advantage of the ongoing crisis.¹³

The importance of context

The question of whether or not a victim should be considered vulnerable is an important question when considering APP fraud. The Financial Conduct Authority (FCA) defines ‘vulnerable customers’ as those that are “especially susceptible to harm” and recognise that one of the key drivers of this susceptibility can be significant life events such as bereavement, job loss or relationship breakdown.¹⁴ The CRM Code has a definition of vulnerability that is more tailored to scams. It sets out dynamic factors as well as the personal circumstances of the individual including the timing and nature of the APP scam itself, the capacity the customer had to protect themselves, and the impact of the APP scam on that customer.¹⁵

Our research would corroborate that it is both the personal circumstances of an individual and how the type and nature of the scam interacts with this that causes someone to be especially susceptible. For instance, we saw how Lyla’s financial distress meant she was open to the investment opportunity and the promise of quick returns that appeared to be sent to her from her sister. Lyla was feeling stressed, tired and in need of extra financial support.

But we have also seen how the accumulation of everyday stresses – exams, a busy work schedule, or loneliness – can also push victims to the limits of their window of tolerance and impede decision-making.

In doing so, they may also make us more susceptible to fraud. Scammers make many approaches to consumers. When they find someone in a distracted and vulnerable state, they exploit the opportunity ruthlessly.

This nuanced understanding of scam victims’ experiences suggests that in setting expectations about reasonable consumer behaviour in the face of fraud, we need to consider a wider range of contextual factors. This means further embracing the FCA’s recognition that vulnerability is contextual, alongside the CRM Code’s more tailored guidance on the nature and impact of the scam. Further guidance by regulators on how firms should implement a reimbursement obligation may be needed to take into account these wider contextual factors and the individual’s window of tolerance. A person should not be held responsible for making unwise decisions or not thinking clearly in a situation where it was incredibly difficult for them to do so.

Fraudsters are opportunistic. Many of their attempts will fail, and often seem laughably clumsy when we are relaxed and able to spot them. But when we are distracted, busy with the stress of life, our limited capacity lowers our defences against scams.

¹⁵ Lending Standards Board (2022), Contingent Reimbursement Model Code for Authorised Push Payment Scams, p.15
Chapter summary

• Many of the victims we spoke to were already **busy, stressed, exhausted or otherwise distracted** when they were contacted by a scammer.

• Being acutely distracted meant victims were already **nearing the edge of their ‘window of tolerance’** when contacted and so the additional stressor meant they became more susceptible to the scam.

• During the Covid-19 pandemic, people were more likely to be stressed and distracted, and this may partially explain the increase in scams seen during this period.

• Understanding these contextual factors and the individual’s position within their window of tolerance is critical to understanding whether there has been evidence of exceptional circumstances that would mean that a victim should not be reimbursed. A person should not be held responsible for making unwise decisions or not thinking clearly in a situation where it was extremely difficult psychologically for them to do so.
2. The scam

Periods of stress and distraction can create opportunities for scammers. But to succeed in defrauding an individual, scammers must engage with their victim and build a credible false pretence for payment to be made.

Our research shows scammers, to be successful, create a credible and trusted persona, for instance, a bank staff member, an investment expert, a seller of goods or a romantic prospect.

Our evidence shows scammers primarily use two tactics to create a credible and trusted persona:

1. **Imitation.** For instance: spoofing a phone number, imitating bank security procedures, or creating credible online profiles and adverts.

2. **Building a relationship** with the victim. The relationship can be romantic or platonic, friendly or authoritarian. To build a relationship the scammer may establish similarities or make themselves likeable.

To understand how these tactics affected the decision making of the victims, it is helpful to reflect on the Wise Mind Model, which describes how we all, as humans, make effective decisions.

The Wise Mind Model is at the core of talking therapies such as Dialectical Behavioural Therapy (DBT) and helps people make sense of why they make certain decisions in life. When applied correctly the Wise Mind Model helps a person reflect clearly on the best course of action to take. Their best decision making comes from their ‘wise mind’.

The ‘wise mind’ is a state where a person’s thinking and decision making is well balanced between their ‘emotional mind’, drawing on feeling and intuition, and their ‘rational mind’, based on rational logic-based analysis.

In our case studies, we routinely saw cases where scammers put victims mentally off-balance by amplifying either the rational or emotional part of their thinking and decision making. Across the cases we reviewed, we saw how scammers can push their victims, through complex cues and manipulation, to act **too emotionally**, ignoring things that don’t make logical sense, or **too rationally**, ignoring an instinct that something might not be quite right, and thus make worse decisions than if they were using their balanced ‘wise mind’.

For instance, to push a victim into disproportionately emotionally-led thinking and decision making, a scammer may build a relationship and then use this against the victim, or as we see in the next chapter, create a sense of urgency or a fear of impending loss. To push a victim’s rational mind, a scammer may spoof a phone number, offer reviews to verify the quality of their product or mimic official procedures like conducting security checks or giving a crime reference number. These are clever short cuts that satisfy the rational mind.

---


In our case studies we identified several key ways in which scammers’ tactics encourage the victim to bypass making a ‘wise mind’ decision. Often, we could identify how these tactics also worked with the grain of unconscious behavioural biases – common features in human decision making, which influence how we think and behave. These unconscious associations, or mental shortcuts, elicit particular responses in particular scenarios. They are crucial to human survival, allowing us to more easily make millions of decisions a day and often helping us avoid danger even when we don’t perceive it.

However, it is also well-understood that these biases mean typical human decision-making is a long way from the perfect rational model. Just as advertisers, retailers, government and other organisations routinely play on our biases in order to increase sales or elicit particular responses, scammers use tactics that work with the grain of our biases to build trust, influence decision-making and ultimately defraud their victims.

**Imitation**

To satisfy the victim’s rational mind, the scammer must appear as the character they claim to be; they must successfully imitate a trusted persona.

One of the most common tools of imitation used by scammers in our sample is **number spoofing**. Number spoofing is where a scammer can impersonate another person’s or company’s telephone number. For instance, a scammer can make themselves appear to be a victim’s bank or a family member. Appearing as an official organisation like a bank feeds the victim’s **rational mind**; logically, the number appears to be from a source they trust. For Aliyah, the scammer appeared to be calling from her local bank branch:

> **Aliyah, 19. Impersonation scam. Lost £1,000. Partial reimbursement.**

Aliyah had just finished her first year of university, and was settling in to enjoy her summer, when she was called from a landline number with a familiar area code. After initially ignoring the call, the number called again, when Aliyah answered she reported the conversation as follows:

> “Hi, I just want to let you know we’re from [Aliyah’s university bank branch].

> Please can you confirm that the number that we’re calling is legitimate?”

> *Bearing in mind I go to university in [place].* He even told me to go on the website to check it was that number.

> I did that and it was the number, so nothing really screams, you know, that ‘this is fake’ because that was the actual number that was calling me... he said: ‘this may be very unexpected, but we have had somebody come into our bank claiming to be you opening a new bank account.’ ”

The scammer successfully convinced Aliyah that it was the bank calling by using number spoofing, and preempted her doubt by ensuring she checked the number was that of the local bank branch early in the call. Pressured by the scammer to quickly ‘protect’ her money, Aliyah sent £1,000 to what she thought was a ‘safe’ account owned by the police.

Another example is Lyla (see chapter 1) whose scammer appeared as Lyla’s sister on Lyla’s phone - the number was the same and so her sister’s name appeared on the messages. Lyla and her sister would regularly speak about finances and was a person Lyla trusted financial advice from. When she received investment opportunities from her sister, this was not completely unusual.

Spoofing the number of a bank works particularly well because it also plays on **authority bias**. Victims are more likely to act compliantly when the scammer appears as an authoritative person, and uses a phone number to verify this.
Victims also commonly told us how credible their scammers sounded. For instance, Oliver says that his scammer, who pretended to be from HMRC, sounded “authoritative” and “formal” – as someone might expect from a tax official.

In other cases scammers imitated ‘official procedures’. Aliyah’s scammer, for example, said he was recording their call as evidence for the police, gave the name of the police officer supposedly in charge and gave Aliyah a crime reference number. For Ruth, the scammer asked a series of security questions as we have come to expect when speaking to our banks. Like spoofing, scammers acting in expected ways feeds the victim’s rational mind, offering a range of logical cues that the call or approach is credible.

We also heard of similar imitation tactics being used online, where scammers are copying the expected online profile of a trusted and credible person. Mark’s story shows even diligent consumers can be tricked when the scammer has successfully created a holistic and realistic profile.

Mark was browsing an online marketplace and he saw a woman selling cheap new tablets and smartphones. “I mean, at first I thought ‘this is rubbish’. “But I started reading the reviews from people, started checking people’s profiles to see who had bought stuff from this seller, to see if they were bots or whatever…. I’ve clicked on everyone’s picture, I followed them and started looking into their lives. I thought ‘you’re a real person’. I even started looking at phones they might be using in the pictures and thought ‘you bought one too’.”

Mark then started questioning the seller to ask for more proof. “The seller sent pictures of boxes of phones. She said ‘this is my warehouse, this is what we do, these are the shipping details, this is the code we used to ship details’.”

Mark also looked up the business address with an online map and clicked on photos of the street to see that it looked like a legitimate business building.

Everything so far has seemed to fit the profile of a legitimate seller: technical details, photos of the goods, good (seemingly honest) reviews and a business building.

Mark said he was still sceptical, but gradually the weight of evidence helped convince him it was real. Mark bought an iPad for £550 that never arrived.

Mark’s scammer successfully imitated the profile of a genuine seller. Mark conducted lengthy and repeated checks for months and the seller appeared to be legitimate: she gave full answers to all Mark’s questions; she sent pictures of the warehouse, receipts, postal tracking IDs, and bank statements. The seller also had many positive recent reviewers who Mark also checked, who Mark described as clearly “real” people. These points of evidence all worked to satisfy Mark’s rational mind, overwhelming his initial instinctive mistrust, to the point where he trusted the seller and made a transfer.

Building relationships
The second main scam tactic identified in our research is building a relationship with the victim to further instil trust. This may be a romantic or platonic relationship, one built on kindness or from a position of authority.

In several cases we found scammers establishing similarities between them and the victim to build trust. Aliyah’s scammer, while talking her through an apparent breach of her bank security, told Aliyah that he had been through a similar experience - and his money had been stolen as a consequence.

“He said this has happened to him before. He was sounding very relatable. He was being friendly. He was laughing when I was laughing.”
Aliyah, 19. Impersonation scam. Lost £1,000. Partial reimbursement.

Aliyah had been pushed into predominantly emotionally-led thinking - she was in shock because her bank account was supposedly under threat. By creating similarities and reassuring her, the scammer was further manipulating Aliyah’s emotional mind. She felt she could trust this man; the scammer was trying to help her.

Katie was seeking friendship online and was initially attracted to her scammer’s similar interests and the fact they had been to similar places like theme parks in Florida.

“There were all these pictures of him in Florida, and I think resonated with me a bit as we had something in common – I’ve been there about 6 times. He said he took his daughter on a regular basis and I used to take my son there…
“I felt amazed that I thought I’d found someone with similar interests to me that had been to the places that I’d been to.”
Katie, 52. Romance scam. Lost £4,000. Reimbursement denied.

Our analysis of case studies suggests that scammers build relationships and establish trust, by manipulating our innate liking bias and similarity bias. Aliyah and Katie felt reassured by the apparent similar experiences as the scammer.

Liking bias is the human propensity to act favourably, and believe the sincerity, of a person we like. If a scammer can build a good rapport with a victim, the victim is more likely to comply with a fraudster’s request.

Similarity bias is where a person will act favourably towards, and believe the earnestness of, a person similar to themselves. If a scammer can establish similarities between them and the victim, whether true or not, the victim is more likely to fall prey to the scam.

Kevin was emotionally fragile when he met his scammer, and again, a range of apparent similarities fostered a quick, emotional bond which opened space for the scammer to defraud Kevin.

20 Imperial College London (undated), Unconscious bias. Available here: https://www.imperial.ac.uk/equality/resources/unconscious-bias/
Kevin, 59. Romance scam. Lost £550. Reimbursement denied

Kevin divorced five years ago when his marriage of 10 years came to an end. After three years of feeling lonely and emotionally stuck, he felt ready to meet someone new.

Kevin joined a major dating site and started talking to a woman from Chicago, USA. He says they emailed regularly and virtually everything he said he liked, she also liked: 80s indie music, classical music, 60s British movies, their favourite travelling destinations.

He says he was doubtful but tried to test her on this knowledge, for instance with obscure 80s indie bands, but she always seemed to have the answer.

“I can't overemphasise, every time I said I liked something, she liked it as well. It is probably what a sociopath does. They're leading you on, they're grooming you. But I was still emotionally and mentally fragile from the divorce. I think that's what they play on.”

Nevertheless, Kevin was still doubtful.

“I said to her ‘Is this genuine?’ And that's when she got really upset over the phone. She said ‘You're making me cry’.”

This made Kevin feel very guilty, especially given the bad previous relationships she said she had experienced - another point of similarity in their stories.

Kevin did other checks, such as ensuring the number she called him on was in fact from Chicago. He ultimately believed their romance to be real and was very upset and embarrassed when, after sending her £550 for a flight to the UK, she disappeared.

Kevin’s story shows how scammers are able to manipulate our natural, human biases to build trust. Kevin did try to use his wise mind - a part of his rational mind felt this might be too good to be true. But the scammer again overwhelmed and manipulated his emotional mind to draw him back in. He was pushed off-balance towards emotionally-led thinking and away from reasoning.

Not all examples are this extreme. For Mark, just one particular product review stuck in his mind:

“I remember one review especially as it was a person like me. He was like my mates. For some reason I think ‘I relate to you’. You know. ‘You're going to tell me the truth because you're like my mate, right?’”


To maintain these relationships and the hold they have over their victims, we found that scammers also purposefully exclude others from the exchange, using secrecy to reinforce trust. For example, in Remi’s case, he was told the offer was a special one, with very limited availability - a way of making him feel chosen, playing to his emotional mind, while also preventing him from consulting others who may have been able to provide a more rational, outsiders’ perspective.

“I kept it to myself because I felt like it was an offer just to benefit me. I was told it was just ten people. So there's no need for me to invite my friends, invite my family or reasons why they should invest in it. So I didn't really want anybody to know.”


In the romance scams we saw, fear of judgement or shame were also reasons why the victims did not mention the romance to others. For instance Francesca anticipated judgement from her family about her burgeoning relationship.
“I didn’t want my family to think I was desperate enough to be with somebody online. My son would have said: ‘well, why are you talking to someone online? You’re not that desperate.’ I think it would have made me think more about whether I was being desperate or not.”

Francesca, 63. Romance scam. Lost £5,000. Did not seek reimbursement.

Authority bias can also make excluding others easier. Aliyah was told by the scammer, who was pretending to be from her bank, to make sure she was alone in the room, as the issue was very sensitive, as though he wanted to protect her.

“He [the scammer] knew somebody was in my room, he said ‘OK darling, make sure nobody’s in your room at this time. Because it’s very sensitive. This is really private.’ So I asked my sister to leave.”

Aliyah, 19. Impersonation scam. Lost £1,000. Partially reimbursed.

Chapter summary

- The scammers began by building trust and credibility with the victims we spoke to.
- The tactics used to build trust and credibility can be broadly grouped as relationship building and imitation of trusted and credible people.
- Relationship building may involve establishing similarities or the scammer making themselves likeable.
- Imitation may involve spoofing a phone number, imitating bank security procedures, or creating credible online profiles and adverts.
- The impact of these tactics on the victims’ decision making can be best understood through the Wise Mind Model. Scammers can push their victims, through complex cues and manipulation, to act too emotionally, ignoring things that don’t make logical sense, or too rationally, ignoring an instinct that something might not be quite right, and thus make worse decisions than if they were using their balanced ‘wise mind’.
- The tactics also successfully trigger unconscious biases in human decision making, in particular: authority bias, liking bias and similarity bias, which impair our abilities to make logical decisions.
3. The payment

The last chapter summarised the techniques we identified scammers in our case studies using to build a credible and trusted persona for themselves. If the scammer succeeds in manipulating the victim thus far, their story has been accepted; in the victim’s mind, the scammer, and the payment they ask for, are legitimate. This final stage in the scam journey aims to push the victim to transfer money to the scammer, while overcoming potential hurdles like bank security features.

Our research shows scammers use two primary tactics to achieve this:

1. Creating an overwhelming sense of urgency. Scammers force victims to feel they must act quickly. This gives the victim little time to double check on what they are being told or seek an outsider’s perspective. This, in itself, can often be enough to overcome doubts and so enough of a trigger to transfer.

2. Coaching and manipulating the victim through the journey to overcome any doubts, or external obstacles such as a bank’s anti-fraud measures or the interference of a third party.

Creating urgency

To induce payment from the victim, the most common tactic in our study was to create a sense of urgency, pushing the victim to act quickly. We found that scammers can manufacture a sense of urgency, usually by creating scarcity or a sense of impending loss. This plays on another set of natural biases, our instinct to acquire scarce, desirable objects and to take quick action in emergencies. While critical to the survival of our ancestors, in the modern world these instincts can lead us to make poor decisions.

Scarcity Heuristic

This describes the human tendency to place greater value on scarce goods or opportunities, which in-turn induces action. People can feel that the deal is ‘too good to miss’ and elicit a ‘fear of missing out’.

In one example, the rarity of the trainers Nadine wanted drove her to act quickly.


Nadine was attempting to buy a rare and expensive pair of trainers. The trainers were typically sold via raffle from the manufacturer, which Nadine missed out on, but were then also resold by individuals. Nadine looked on several different websites but all the trainers were either being sold at hugely marked up prices or on websites she didn’t trust.

Eventually, after searching online and speaking to multiple sellers, Nadine found a pair which she felt were reasonably priced, in a good condition and on a platform she trusted.

The seller asked Nadine to move to a direct messaging app so they could be in quicker communication, which Nadine did. Nadine then asked for more photos and videos of the shoes, to check they were genuine and in good condition, which the seller provided. Nadine then felt reassured that the shoes were genuine and the seller had them to sell.

She didn’t want to miss out on a rare good deal so bought them that day, but the shoes never arrived.

For Sarah and her son, it was an attempt to find the latest PlayStation games console during a global supply shortage which helped push them to act quickly.

**Sarah, 56. Purchase scam. Lost £650. Reimbursement denied.**

Sarah wanted to buy her son a PlayStation 5 but, due to the global supply shortages, they missed the first round of shipments to the UK.

Her son then found a seller on social media, who said he accidentally had two of the consoles as he bought one for himself and his mum had bought one for him too. Given the scarcity of consoles and uncertainty about when they might next be able to find one, Sarah’s son was keen not to lose out on the opportunity to buy it.

“My son texted me first and then he rang me. He knew that if that lad sold it, we would miss out.
So there’s that rush, you know, you’ve got to decide now. I said ‘can’t you wait?’ He said ‘no because they’ll sell it and then we’ll miss it. I’ve looked everywhere else. There’s none in the shop’.”

When she asked questions about the console to test the seller’s legitimacy the seller also began to apply pressure.

“He said something like ‘I’ve got ten other people wanting it. Quick!’.
You know, putting the pressure on to make the sale.”

Sarah says that the seller eventually convinced her by sending photos of the PlayStation, of the receipt for it from a legitimate electronics retailer, and of proof of his address. She also says that the story “added up” because she could see from the photos, from the room he was in and his clothing, that he looked like a “normal teenager” living with his mum, as he claimed to be. This all convinced her that the seller was legitimate.

The urgency created by the short supply and the pressure from the seller, plus providing enough evidence to satisfy her doubts, meant Sarah sent the seller money but never received the console.

Another way we saw scammers inducing scarcity bias in victims was to entice them with an offer that is time-limited. In Adam’s story we saw how a declining global economy meant the investment opportunity felt time-limited as he had to get in before the economy turned worse:

**Adam, 43. Investment scam. Lost £2,000. Reimbursement denied.**

Adam says that he likes to always be prepared, financially and otherwise.

To build financial resilience, Adam sought investment opportunities. Having taken an interest in cryptocurrencies, and hearing about them from friends, he invested lightly to start.

However, the national and global economic situation started to weigh on Adam’s mind, creating a sense of urgency to make more money and become more financially secure.

“I’m [watching videos online] and I’m seeing a lot of things saying ‘the financial markets are going to crash’, ‘the world’s going to go into recession’. So that highlights my urgency. I feel like I’ve got to be quick.”

After searching for more investment opportunities on social media, he found an investor who promised to make Adam money through cryptocurrencies. The investor then also used the changing economic climate to convince Adam he needed to invest urgently.

“He said ‘look, the market’s about to crash, we’re onto a good thing’”

Adam was being compelled to act to avoid potentially losing money in a declining economy.

After having further conversations with the investor, Adam said the final trigger to act was seeing a personal friend’s name associated with the investor, creating a social proof, which Adam said “was the carrots I fell for”.

For Adam, the economic climate made him worry he would lose what he had - his money, his lifestyle and his financial buffer. The way to rectify this was to make more money, and make it quickly.
Adam felt compelled to act quickly because he felt the potential for investment gains potentially slipping away unless he acted urgently. Yet his story is also an example of someone trying to avoid potential losses - he wanted to insure himself against a declining economy. He was also falling into the **loss aversion bias**.

**Loss aversion bias** is the propensity for people to weigh potential losses heavily and thus seek to avoid them.²²

Loss aversion bias means people are more likely to be risk-seeking in order to avoid expected losses, in contrast to people’s propensity to be risk-averse with potential gains.²³ For example, an investor may not sell an investment which is declining in value, in the hope that it will rise in value in the future, to try to avoid the loss.

In effect, humans are more likely to act rashly or with greater urgency, if they anticipate a potential loss – whether this loss is explicit such as the threat of theft, or implicit such as a declining economy.

Ruth was tricked by the scammer into thinking her money was under threat and needed ‘protecting’, like Aliyah in chapter one. Ruth was told ‘scammers were out to get her money’. This played to Ruth’s bias of loss aversion which made it easier for the scammer to compel Ruth into acting quickly to avoid a potential loss.

Ruth, 54. Impersonation scam. Lost £9,000. Fully reimbursed.

On a Saturday afternoon while her sons were at university, Ruth received a call from someone claiming to be from her bank’s fraud department, stating that her account was under threat. In order to protect her money, she needed to send it to a safe account.

Ruth was initially dubious. The scammer wanted to go through a series of security questions, mimicking the process of her bank. When Ruth asked “Well, how do I know that you’re not fraudulent?”, the scammer listed transactions she had made in the last few days. “And so I thought, okay, you’re obviously legit.”

Ruth said she was calm. She felt the bank had the situation under control, was acting in her best interest, and the staff member she was speaking to was reassuring. The scammer had also supposedly booked a meeting for her in the bank branch on the Monday coming, which she said she felt comforted by - as any questions or doubts could be raised in the meeting.

The scammer first elicited a sense of urgency in Ruth by manipulating her through the loss aversion bias – her money was under threat and she felt she had to act quickly. Then they reassured Ruth by creating a credible and trusted bank staff persona (asking security questions; listing her recent purchases), and seemingly being kind (telling her it would be okay, her money would be safe). By satisfying her rational mind by mimicking bank staff, and overwhelming Ruth’s emotional mind – through urgency and calming reassurance, Ruth quickly trusted this man, believed he was from the bank, and so transferred her money into a ‘safe account’.

Only when she went into the bank on Monday and there was no appointment, did she realise it was a scam.

The case studies in our research consistently show that by manufacturing a sense of urgency, a scammer can invoke loss aversion or scarcity bias, overwhelming rational judgement and compel a victim to make a payment. Combined with tactics that build trust and credibility, as seen in chapter 2, urgency can reduce the victim’s ability to question what they are being told and can mean they are more likely to send money to a scammer.

---


**Scammers coach and manipulate a victim through the payment**

Banks have invested heavily in systems to try to protect people from being scammed at the point of payment, and have terms and conditions with customers that allow payments to be delayed if there is a reasonable suspicion of fraud. Sadly, however, our research demonstrates that scammers can manipulate their victims in ways that reduce the efficacy of these systems.

In some of our case studies, successful scammers understood and anticipated the potential obstacles they may face to securing payment. These included external barriers, internal doubts from the victim, and the influence of third parties (see chapter 2).

We saw evidence of scammers successfully coaching victims to bypass bank’s anti-fraud measures, while maintaining their trusted personas and the integrity of their victim’s beliefs. Aliyah’s scammer, who was convincingly mimicking her bank, telling her that someone was trying to hack her account and telling her she needed to move her money to keep it safe, encouraged Aliyah to pay in instalments. This allowed the scammer to bypass Aliyah’s bank’s transfer limits. But in the way the scammer described this, he also twisted the scenario to further ingrain his position as the bank in Aliyah’s mind.

“He told me it’s better to transfer in instalments so the hacker doesn’t know I’m withdrawing the money … When I was paying him, he said there’ll be a warning but he’d take it off for the next instalment. But that’s just what happens the next time you pay the same person repeatedly. So he fooled me, making it seem as if he has control of my bank account.”

**Aliyah, 19. Impersonation scam. Lost £1,000. Partially reimbursed.**

Ruth’s scammer was also well versed in how her banking worked, guiding her through the payment process, including through the fraud warning.

“He’d say: ‘OK, this is going to come up now you need to press yes, then another screen will come up.’

“So I do that and he goes: ‘Does this come up? Yeah. OK. Right. Next one.’

“So we went through a number of screens and he always knew which was going to come up and he told me what I had to do for each one.’

“When the warning came up asking if I was sure I wanted to send the money, he talked me through it, he said something like: ‘so this warning is going to come up now. We need to override that. So you need to do these things.’

**Ruth, 54. Impersonation scam. Lost £9,000. Fully reimbursed.**

Bella’s scammer told her to use a generic payment reference, to avoid any potential suspicion from her bank or from others. She felt they were acting in her interest – not wanting her to miss out on the investment opportunity.

“They said to me ‘you shouldn’t mention coin or crypto in your description of payment. In some countries they are yet to legalise trading of cryptocurrency, while in some there are some regulations that curtail trading crypto, which we can’t be sure of.’ “

**Bella, 29. Investment scam. Lost £7,750. Reimbursement denied.**
Warnings at the point of payment won’t always stop the scam

So far, we have seen how a scammer can successfully trick the victim into believing the scammer is trustworthy. By catching victims at inopportune times, by using impersonation, building trust, playing on psychological biases and creating urgency the scammer has successfully led the victim to the point of payment.

At this stage, for the victims we spoke to, their belief in the scam was complete. Even when third parties questioned the victims about what was going on, or when the victim themselves questioned the scammer, doubts were quickly pushed aside.

“I said to the scammer ‘Well, how do I know that you’re not fraudulent?’ and he said ‘That’s a really good question. Let me just go run through some of the things that you’ve been spending on your account for the past few days.’ He did, so I thought, okay, you’re obviously legit.”

Ruth, 54. Impersonation scam. Lost £9,000. Fully reimbursed.

“When I was at the bank I’m sure the cashier said something like ‘are you sure it’s genuine?’ But at the time I was sure it was my daughter”

Susan, 64. Impersonation scam. Lost £2,200. Fully reimbursed.

This does not reflect excessive credulity on the part of the victim, but rather the natural progression of human decision making. When we come across information that conflicts with our accepted internal narrative, we often struggle to engage with it. This is known as ‘cognitive dissonance’.

Cognitive dissonance describes the state of mental conflict or discomfort when a person tries to hold two conflicting thoughts at the same time, or when a person’s actions do not align with their thoughts or beliefs.\(^{24, 25}\)

For instance a person may believe and internalise the negative health effects of smoking, yet continue to do so by changing their thinking or seeking to ‘justify’ their smoking. They may emphasise their enjoyment of smoking or de-emphasise the risks. They are trying to reduce the discomfort of cognitive dissonance – of knowing smoking is bad for their health but continuing to do so.

A victim’s failure to act upon their doubts, therefore, does not reflect a lack of care, but the success of the criminal behaviour of the fraudster, who has created a situation where the victim is unable to tolerate doubt. It is not the victim choosing to ignore information or instincts, but rather them being unable to sit with conflicting information and seeking prompt resolution of their discomfort.

Chapter summary

• This final stage in the scam journey aims to push the victims to transfer money to the scammers.

• For this, scammers had two primary tactics: **creating an overwhelming sense of urgency** and **coaching the victims through the payment process**.

• **Urgency** can usually be created by employing **scarcity** or **a sense of impending loss**, which creates pressure in the victim to act. These play on the unconscious biases ‘scarcity heuristic’ and ‘loss aversion’ making them more likely to succeed.

• **Coaching the victim** means scammers walk victims through the journey to **overcome doubts or external obstacles** such as a bank’s anti-fraud measures or the interference of a third party.

• For the victims, **warnings at the point of payment weren’t effective in disrupting the narrative they had accepted about the scammer and the payment.** This is because they may have believed the scam to be true, they trusted the scammer or they felt otherwise compelled, forced or unavoidably obliged to pay their scammer. Doubts were often pushed aside because conflicting information – between doubts and belief that the scam was true – was psychologically uncomfortable to hold.
4. The aftermath

The final part in the journey of a scam is the moment the victim realises they have been defrauded, and their efforts to deal with the consequences. The sums involved can be significant and it can be difficult to come to terms with being deceived. This had three common consequences on the victims we spoke to:

1. Realising they had been scammed was highly distressing
2. Dealing with their bank or other institutions can add further distress
3. Decisions and actions by banks and other financial institutions were not felt to be clear enough

The aftermath of the scam is important because the outcomes for victims, and how they were treated in the process, often proved significant in determining how the victims felt in the long-term. Those who received their money back or had better experiences with authorities felt better, compared to those who were left dissatisfied as they had not received their money back or felt unheard.

Realising you have been scammed is highly distressing

The victims we spoke to often said the moment they realised they had been scammed was hugely upsetting. Victims told us they felt ashamed, angry or betrayed. Some hid the scam from loved ones, particularly if the amount of money was significant or did not only belong to them.

In some cases, victims then doubted themselves and their own financial acumen, their ability to find love or in their judgement more broadly. Others turned to anger and fantasised, for instance, about catching the scammer. At a time when many were already stressed and overloaded, being scammed is another burden many struggle to cope with.
“I realised: ‘Oh my God. I have been scammed. I just cried and cried … I came home and felt awful: so stupid, embarrassed, ashamed and every sort of negative emotion you can imagine. I thought: ‘I can’t tell my dad because he’s just lent me a lump sum of money and I’ve lost it.’ I went round to talk to my sister – she’s the only person I told everything to.”

Ruth, 54. Impersonation scam, Lost £9,000. Full reimbursement.

“It felt like someone had died. It was a massive shock that the person I really liked would disappear like that. It was financial of course, but at the start it was the shock of losing him - it felt like a bereavement. I didn’t sleep for 24 hours afterwards. I didn’t eat. This made me feel ill. I couldn’t function. I had to phone in sick to work.”

Katie, 52. Romance scam. Lost £4,000. Reimbursement denied.

“It’s a combination of rage, bitterness, embarrassment, stupidity. I’ll be honest I cried my eyes out for about an hour when I realised.”


“I passed over finances to my husband because I felt more scared of having a mishap. It’s frustrating because I prefer to deal with everything myself”

Lyla, 41. Impersonation scam. Lost £3,000. Reimbursement denied.

“I was very angry. I was very down for a good couple of months. I was frustrated because I couldn’t do anything about it. I felt like I couldn’t tell anyone as well. I think that was the worst thing about it – having to go through it alone. I felt ashamed. Those kinds of emotions went through me all the time. I felt if I told anyone I would be judged a lot. I thought people I know, my family, would say ‘you stupid girl’.”


“No longer save. I’ve lost interest in saving for anything. If I buy things and I have something left, that’s cool. But consciously planning to save for something, I’ve not been able to do that.”


Some of the victims we spoke to delayed telling authorities and seeking reimbursement, and two did not seek reimbursement at all. When they did, it was common for victims to feel frustration at their bank or other institutions involved in helping them seek redress.

**Dealing with the bank and other institutions can add further distress**

Once victims approached their bank, to inform them of what happened or to seek redress, they reported feeling confused and disheartened by the process. Some of the victims we spoke to felt the bank was unsympathetic or not clear in how they reached a decision on reimbursement. Some also do not understand what happened to their money, thinking that the transaction can simply be cancelled or reversed. In total this can leave victims more upset.

Ruth’s example shows a system eventually working but taking too long to get there and with significant hurdles for the victim. Ruth had to fight her own corner after being the victim of a crime. In the meantime, the delay to her reimbursement left Ruth in a position of financial difficulty.
Ruth, 54. Impersonation scam. Lost £9,000. Full reimbursement.

Ruth realised she had been scammed in her local bank branch, expecting to have a meeting which was booked by a scammer. When this turned out to be false, she burst out crying.

The bank manager tried to call their fraud department for her. Ruth says the manager could not get through that day or for the entire week. A couple of days after he eventually did get through, Ruth was told by her bank she would not receive reimbursement, though she did not understand why she was denied the money.

“I got an email a few days after the manager got through from the fraud department saying:

‘We understand this has happened, there isn’t really anything we can do’

“I thought you’re not even giving me a chance to explain. It was almost just a straight ‘no’.

Afterwards, I would read things and think: ‘hang on, apparently banks have money to give back to people when this has happened. Why are you not giving it to me?’ “

She wrote back to the bank arguing her case, and they replied saying that if she did not like their decision, she could go to the Financial Ombudsman. The Ombudsman took on the case, but she did not receive a final decision for nine months, despite repeatedly chasing. Eventually, she was told she would be reimbursed, and received the funds within two days.

When talking about those nine months, Ruth said:

“The thing is, I live on benefits so I don’t have any money. Not long before it [the scam] happened, my dad had lent me money and so I had a few weeks of not worrying about bills, but then suddenly I was back to worrying again … I couldn’t tell my dad because I was too ashamed.”

Others spoke about their bank’s lack of empathy or experience with their situation. They felt vulnerable and embarrassed. For instance, Kevin said speaking to the bank was one of the most embarrassing experiences of his life and he felt too ashamed to pursue the case further after being told he would not receive reimbursement.


Having found out that his online romance was a scam, Kevin reached out to this bank:

“I spoke to the scams department and they said ‘Can you send us some of the emails you sent to her and she sent to you?’ I found that difficult to do. I only found one or two emails that I could send because they’re personal. I did send them and they said:

‘I’m sorry, you’ve left it too late. If you’d have told us immediately, we might’ve been more sympathetic.

From these emails you’ve given us, we can’t confirm that it is a scam. Because we’re not 100% sure and because you’ve left it too late, we can’t help.’

“It was embarrassing. Humiliating. The phone conversation with my bank was probably one of the most embarrassing moments of my life. They said I could go to the Financial Ombudsman but didn’t want to because I felt too embarrassed. I didn’t want to write to another organisation telling them somebody told me they loved me and I fell for it. I think the scam relies on that too. They know you’re not going to follow it up because you’re too embarrassed. So, I didn’t follow it up with the Financial Ombudsman. I left it with my bank and they said no.”

When asked what he thinks banks should understand about situations like his, Kevin said:

“They need to understand that people are going to be embarrassed in mentioning the scam to them in the first place. They might hesitate in contacting them because they’re too embarrassed and humiliated.”
Decisions and actions by banks and others are not being explained clearly enough

Other victims couldn’t understand why the bank wouldn’t simply give them their money back as would happen with unauthorised fraud. Even at the time of interview victims were still unclear as to why the transaction could not be stopped. Ian believed that because he had a direct debit cancelled previously then this payment could be cancelled too, and didn’t then receive a sufficient explanation on what was happening.

“I explained to my bank the situation and they're like ‘Well, as you've sent it knowingly, there's nothing we can do about it’. I said: ‘Well can't you just reverse the payment? Stop the payment going through. I think it's been fraudulently done. Just stop it.’ My bank said: ‘No, we can't Mr.’

Well, why not? Why not just pull the payment? I know that there’s a way of pulling the payment back. Years ago, I had an argument with [a telecommunications company] over something and I paid a monthly payment, and I got the bank to stop the payment. And I thought well why not this time?”

Ian, 48. Romance scam. Lost £250. Did not seek reimbursement.

Presumably in these cases where reimbursement has been denied, the bank has made a judgement that the customer has met one of the four exclusions for reimbursement in the Contingent Reimbursement Model Code. If this decision is made, we would expect it to be clearly explained to the customer. The lack of clarity on the reasons for being denied reimbursement amongst the victims we interviewed suggests, at least, that these reasons are not being clearly explained to customers. Worryingly, this would prevent them understanding that in these circumstances they would have the ability to appeal the decision to the Financial Ombudsman, which frequently finds in favour of scams victims.

“No, I don't think they did give me an explanation on why I got my money back. They just said ‘under the circumstances, we can reimburse you.’ The bank were very good, they didn't make me feel stupid. But I was surprised I got my money back.”

Susan, 64. Impersonation scam. Lost £2,200. Fully reimbursed.

“[the payment provider] had all the answers. I don't expect them to give them to me because of data protection. I get that. However, they should be able to give them to the police or to some other governing body”.

They just said there was nothing they could do. They didn't explain any appeals process.”


“The bank wasn't really supplying much information. Sometimes I was the one that stopped them and asked for information. I also felt like they weren't really friendly, they weren't trying to be responsive. I made a mistake myself but I wanted feedback – should I have involved them before making the transfer? They didn't really tell me. They just said nothing could be done. ”

[Interviewer asks whether the bank told him he could speak to the Financial Ombudsman]

“No no, they didn't at all”

Chapter summary

• **Realising they were scammed was an extremely distressing time for victims.** Emotions ranged and oscillated between shock, anger and anguish. Many also described feeling highly ashamed at being tricked and losing significant amounts of money, which was occasionally shared or borrowed from loved ones.

• **Banks, the police and other institutions were often felt to have not dealt with the situation well.** Victims felt unheard, misunderstood, uncared for or blamed.

• **Victims also often said, or indicated, that they did not fully understand the decisions of their bank, particularly regarding reimbursement.**
5. Recommendations

Our research sought to understand the journey of an APP scam in detail, to explore how people fall victim to scams, and the extent to which people can reasonably protect themselves. By analysing our case studies using psychological frameworks, we have attempted to explain why scams are so seductive, and how people fall victim. We found that victims often fell prey to scams when they were already stressed, busy, tired or otherwise distracted. They were emotionally overstimulated which made navigating a sophisticated and opportunistic scammer much more difficult.

We also found that during the scam itself, the scammer has two sequential strategies. The first is to build trust and credibility in the mind of the victim. This is done through imitating a trusted and credible person or institution and through building a relationship with the victim. The second aim is to push the victim to make a transfer of money, which can be induced by creating a sense of urgency and by coaching the victim through the payment. These tactics make it very difficult for the victim to identify that they are being scammed, or to take action to protect themselves. Yet many of the victims that we interviewed, across a wide range of types of scams, were denied reimbursement.

What do our findings suggest about how we can prevent scams from happening in the first place? And, given that we will not always be successful, how should we respond once a scam has taken place?

Consumers are put in harm's way by a myriad of weaknesses in everyday systems – social media platforms hosting fraudulent adverts, online marketplaces selling fake goods, telecoms companies allowing scammers to spoof numbers and banks allowing fraudsters to operate accounts. Despite these wider enablers of fraud, consumers are all too often left to themselves to prevent becoming a victim or to shoulder financial losses.

We could continue to put much of the onus on individuals to protect themselves from becoming victims and to shoulder financial losses. However, while some scams may be prevented this way, our findings show that such an approach is unlikely to be effective on its own and it is not fair. Victims do not set out to be scammed, and the way in which scammers manipulate normal, human behavioural biases makes it incredibly difficult for people to spot a scam in action.

Instead, we need a system-wide approach to stop the source of scams. This should aim to prevent scammers from reaching victims in the first place, to maximise the chances of disrupting a scam in progress, and to ensure consumers are not held accountable for the criminal behaviour of scammers with adequate support and reimbursement. Individuals need to play their part too to help these systems prevent fraud, but this needs to be rooted in a better understanding of how fraudsters manipulate their victims and the psychological factors that mean consumers cannot be expected to consistently protect themselves against scams.

A fairer system of redress

Too many consumers are being let down by the voluntary APP scam reimbursement scheme. Currently, there is a lack of systematic oversight of the way the scheme is implemented.
The banking industry has a financial incentive to act stringently with the reimbursement of victims but the industry is also, in effect, both judge and jury. The insufficient reimbursement of victims suggests implicitly that victims themselves are to blame for the scam. This is no surprise given that the term ‘blame’ is baked into the voluntary reimbursement code, with the banks involved in the payment tasked with deciding whether the victim – and their own firms – were to blame or not. This misses the point. It is only the criminals that are to blame. We must ensure new regulations do a better job of giving justice to victims. Theoretical concerns about potential ‘moral hazard’ from raising levels of redress for victims do not appear to be borne out from TSB’s experience\(^\text{26}\) from its Fraud Refund Guarantee.\(^\text{27}\)

Despite ten major firms signing up to a voluntary reimbursement code for APP scams, victims still shoulder two-fifths of reported losses.\(^\text{28}\) The PSR has concluded that reimbursement levels have been significantly lower than it expected when it proposed the voluntary reimbursement code. Since 2019/20, the Financial Ombudsman Service has upheld around three quarters of complaints by victims against banks for authorised fraud, compared to an uphold rate for all types of complaints of around a third.\(^\text{29}\)

We welcome the Government’s Financial Services and Markets Bill which requires the Payment Systems Regulator to make reimbursement mandatory for qualifying Faster Payments transactions. This new approach could significantly reduce the financial and related emotional impact of this form of fraud on victims if it leads to fairer decisions by those already reimbursing their customers voluntarily and those firms that do not currently reimburse victims. However, this change will only have that effect if it reflects how victims are manipulated by fraudsters and covers all payment service providers. By providing a direct financial incentive on all 400+ payment service providers to prevent APP scams, it could also help drive better preventative and reporting measures.

While the Faster Payments scheme is the urgent priority, given that it makes up the vast majority of APP scams that we currently have data for, this could evolve relatively quickly as fraudsters change their approach. We therefore also want to see action across a wider range of payment methods.

We recommend that:

- **The Payment Systems Regulator should proceed with its proposals for a reimbursement obligation for all payment service providers that:**
  - **Applies in all but exceptional circumstances** – providing a clearer and fairer basis for reimbursement than under the existing voluntary reimbursement code. Our research demonstrates that when consumers are scammed, it is not because they are acting irresponsibly. In our case studies, we found people who had questioned what they were told, but their normal behavioural

---

\(^\text{28}\) In H1 2022, 60% of losses were reimbursed to APP scam victims under the CRM Code, totalling £117.2 million. See UK Finance (2022) 2022 Half year fraud update, p.22. Available at: https://www.ukfinance.org.uk/system/files/2022-10/H1alf%20year%20fraud%20update%202022.pdf.  
bias, in combination with the manipulative behaviour of fraudsters, made it impossible for them to see through the scam. The expectations of consumer behaviour to merit a judgement of exceptional circumstances, and refusal to reimburse, must be based on a reasonable understanding of normal human behaviour and psychology.

**Fully protects victims who were especially vulnerable** – who are least able to protect themselves and to cope with the financial and emotional impact of fraud.

**Covers all types of APP scams** – given how similar the techniques used by fraudsters are across different types.

- **The Government should legislate so that scam victims can take action to enforce their rights directly against firms that are in breach of these obligations.** Whilst supervision, enforcement and oversight by the PSR will be critical overall, individual consumers may not always be treated fairly and in line with the law in practice. As well as consumers having access to the Financial Ombudsman Service, the Government should therefore introduce additional effective legal mechanisms for cases where a breach of the reimbursement requirements has occurred.

- **The PSR should provide regulatory oversight of the new reimbursement obligation and take enforcement action against firms that do not meet its expectations.** This will help to address the challenges with the implementation of the current voluntary reimbursement code. With approximately 400 payment service providers coming under this new obligation, consistent outcomes will be even more challenging to achieve so close regulatory supervision and clear guidance will be needed from the outset.

- **The Payment Systems Regulator should require all payment service providers to report and publish data on APP scam levels and reimbursement.** The PSR has proposed this for just the largest 14 banking groups and for a limited set of information, which could provide a partial and misleading picture. It should instead extend these proposed requirements to all payment service providers, and require firms to include data on the time taken to resolve complaints and the stage at which complaints were resolved, including data from the Financial Ombudsman Service. Taken together, these improved measures would help to ensure that the mandatory reimbursement obligation is implemented consistently by publicly highlighting potential issues and helping to drive better approaches among firms.

- **The Government should carry out a broader review of consumer protections for different payment methods.** The Government is right to prioritise action on reimbursement for the Faster Payments Scheme, where most reported APP scams currently take place. We also want the PSR to consider further measures on the seven other payment schemes which it regulates. Despite significant innovation and change in the way consumers make payments in recent years, just one payment scheme has been added to the PSR’s remit since it was established seven years ago. HM Treasury should consider whether the list of designated payment systems should be extended. It should also conduct a review of consumer protections for other payment methods, many of which are via payment platforms like e-wallets and cryptocurrency platforms, rather than just payment systems that could be regulated by the PSR.

**More effective support for banking customers**

It is not just that victims are left out of pocket by fraud, they are often also let down in terms of how they are treated. Banks and other payment service providers are often where victims of APP fraud turn first when they discover that something may have gone wrong. They can then be subjected to difficult and embarrassing conversations about their actions, as firms try to find out what has happened and consider how to respond. Too often victims are made to feel like they are to blame.
This is not only harmful in and of itself, it is also a missed opportunity to fully understand the circumstances of the scam to help support a customer to prevent them becoming a victim again and to help prevent others from falling victim. This victim blaming can also create an adversarial relationship between bank and customer, which can harm attempts to prevent fraud that require customers to respond to interventions from their bank. Seeing customers more as partners in the fight against crime can help the banking industry to unlock more effective measures to prevent fraud as well as a more supportive relationship with customers that are victims of fraud.

In recent years, the banking industry has introduced new warnings prior to payments being made, which are often tailored to the purpose of payment. Many banks have introduced Confirmation of Payee, a vital name-checking service. Taken together, these two interventions can significantly help to prevent scams. However, consumers are bombarded with communications all the time, so there is a general risk of these warnings being ignored, especially if they become routine. Our findings also highlight the specific risks from fraudsters coaching their victims around warnings.

More targeted interventions require industry to share better information on fraud risks. A system for payment firms to share data about sending and receiving accounts at the point of payment is being developed by the banking industry. This could have a significant impact but only if it is adopted across the industry. We believe this should be mandatory when it’s ready, based on the recent experience from similar industry initiatives such as Confirmation of Payee that has required regulatory intervention. This better assessment of fraud risk would help firms to ramp up interventions where they are most needed. There also needs to be better testing of what works, so that preventative measures evolve and respond to the changing fraud threats.

We recommend that:

- **All payment service providers should train relevant staff on how to support victims of APP fraud.**
  
  The Lending Standards Board has previously found that among the 10 signatory banks to the voluntary reimbursement code, across many examples there was a lack of understanding of the Code by frontline staff and in some cases a lack of understanding of internal claim investigation processes led to extended wait times and poor customer outcomes. The PSR’s proposal for a reimbursement obligation for payment service providers would mean that all vulnerable customers should be reimbursed. This will require firms to carefully understand their customer’s circumstances and what has happened during the fraud. With almost 400 payment service providers offering bank transfers that have not been subjected to this scrutiny of how they train staff, there is a significant challenge here for the industry to meet. Without proper training, vulnerable customers risk being overlooked and lacking the wider support needed to help them recover and to avoid becoming a victim again.

- **All payment service providers should be required by the Payment Systems Regulator to share standardised data with each other on fraud risks before making a transaction.** New standards and processes are currently being developed by an industry working group that seek to enable the sending and receiving payment provider to exchange key information on the customers involved in the payment. This could include the type and age of accounts being used and the purpose of the payment. This information could alert the payment providers to suspicious payments, meaning that efforts to prevent fraud could be better targeted. We want the PSR to make sure these standards are implemented by all payment service providers, as fraudsters will simply target weak points if this is not the case.

---

• Payment providers should continually test and improve the effectiveness of their customer fraud warnings and consider other risk-based interventions. Tailored fraud warnings at the point of making bank transfers have been introduced by many providers in recent years. This is a welcome step but these warnings need to evolve based on the evidence of what works. Consumers are bombarded with communications all the time, so there is a general risk of these warnings being ignored, especially if they become routine. Our findings also highlight the specific risks from fraudsters coaching their victims around warnings. Firms should carefully consider how they interact with their customers to prevent fraud, including considering other interventions, beyond online warnings, for suspicious and higher-risk payments. This could include delaying payments and speaking directly with their customers, which could help identify where customers are experiencing cognitive dissonance, and expose gaps in the scammers’ stories. The biases we showed that scammers exploit in this report could form the basis for further preventative engagement with customers, for example exploring the role of similarity bias, loss aversion or scarcity.

Tackling wider weaknesses

Fraudsters exploit weaknesses in the systems that consumers interact with in their daily lives, from their communications with businesses, friends and family and even potential romantic partners, the marketing they are exposed to, and how they bank and make payments. To turn the tide of fraud, in addition to improving reimbursement for victims and more effective support for banking customers, we also need to take steps to prevent fraudsters reaching their victims in the first place, whether that is through a spoofed number, an online platform, or fake advert.

The UK has a number of laws to tackle scams including wide ranging fraud legislation, strict regulation of the advertising of financial products and legislation to protect consumers from misleading adverts. However, outrageous levels of fraud suggest that these rules are routinely breached and not sufficient to protect consumers. The wide range of firms that fraudsters use to reach and manipulate their victims need to have clear legal responsibility for tackling fraud, with harsh penalties, including fines, for those that fail to meet these responsibilities.

Better reporting and data sharing is also crucial to catch criminals in the act, halt the movement of funds before it's too late and to prevent fraud in the future by spotting patterns of behaviour and potential weak points. As it stands, the systems for consumers to report fraud and for industry, policymakers and law enforcement to share data are ineffective and siloed. Victims who try to report scams too often tell us that they felt judged and did not receive the support they needed, disincentivising future reporting. We need to make it easier for consumers to report scams and get the support that they require. Better reporting also opens the door for this information to be shared between stakeholders as necessary to prevent fraudulent behaviour, wherever that may occur. For example, online platforms could be enabled to alert banks to fraudulent accounts.

Action is needed across industries to address these weaknesses. We recommend that:

• Ofcom should ensure that all telecommunication providers offer the same protections to consumers to prevent number spoofing. We welcome Ofcom’s plans to introduce technical standards to allow networks to confirm the authenticity of a number before a call is made. This has the potential to reduce the risk of scams from spoofed numbers and improve consumer confidence and trust. In order to realise the possible benefits, Ofcom must ensure that the same protections are offered by all telecoms providers.

• **The Government should pass an improved Online Safety Bill into law to prevent users from encountering fraudulent content online.** The Online Safety Bill proposes duties on online platforms including search engines, social media and dating apps, to prevent users from encountering fraudulent user generated content and fraudulent advertisements. Currently far too many consumers are harmed by fraud online, as our recent report on fraudulent investment ads exposed. The Bill’s duties will ensure that platforms have proportionate processes in place to protect them. While there is room for improvement in the current Bill, it is crucial that legislation is introduced to tackle fraud online as soon as possible.

• **The Government must do more to help facilitate effective data sharing and reporting systems across industry and regulators to tackle fraud, and empower consumers to report scams.** Existing legislation clearly allows data sharing for the purpose of fraud prevention and the Government can do more to encourage businesses across sectors to do so. Regulators could also do more to ensure that the data they hold, such as the FCA warning list, are held as open data that can easily be incorporated into external systems. Further to this, the Government should work with the different industries where consumers experience fraud, to ensure that they have effective reporting mechanisms that support consumers in reporting scams. The proposal in the Online Safety Bill that instructs online platforms to have easy to use processes for reporting fraudulent content is the first step in supporting effective reporting systems that empower consumers. This data must then be effectively shared with relevant industries, regulators and law enforcement to help prevent consumers from being harmed again by the same scam tactic.

---

32 Which?/Demos Consulting (2022), *Capital at risk: How platforms can do more to tackle misleading and fraudulent adverts online*
the psychology of scams – understanding why consumers fall for app scams