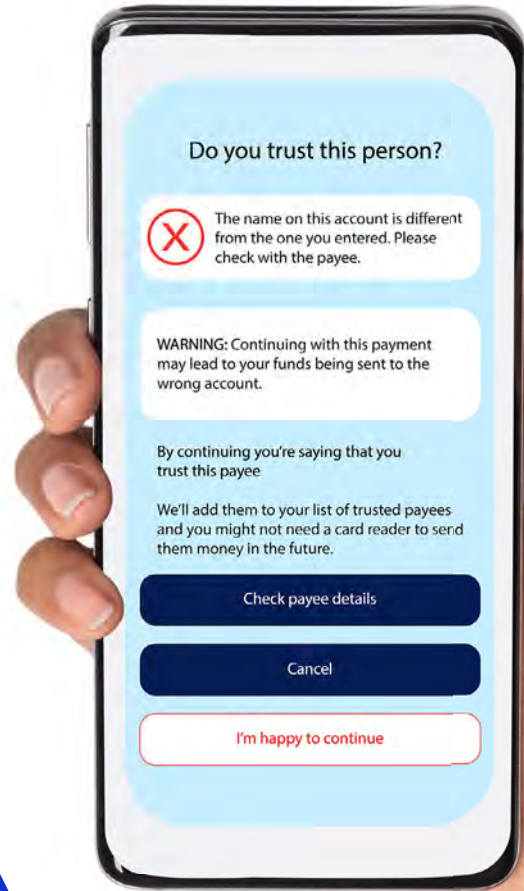


# The impact of APP scams

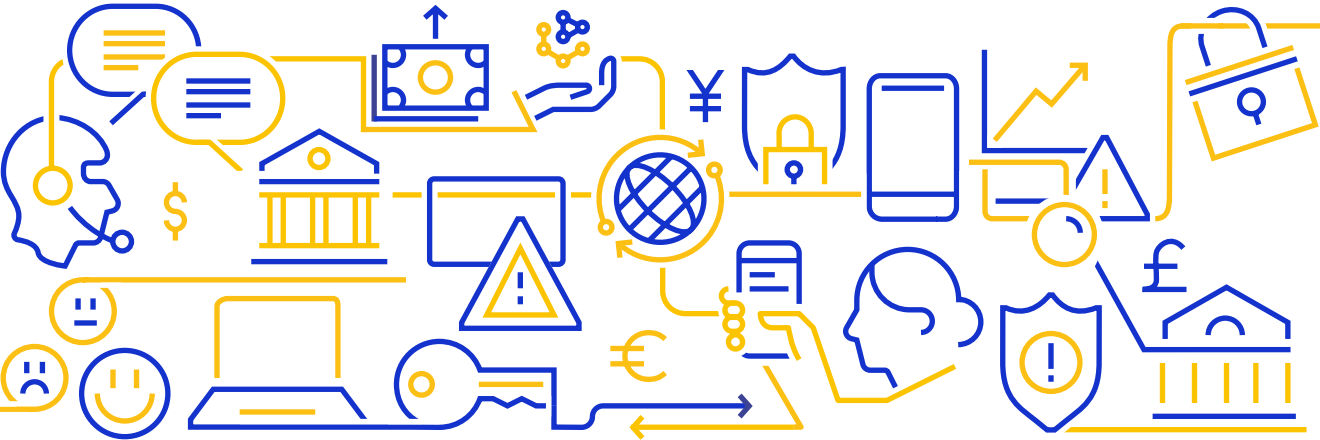


Visa's insights and solutions can provide a **safer future**



# Contents

- Executive summary 3
- Market context 4
- Chapter 1: APP scams, a hidden threat 5
- Chapter 2: Discovery and resolution 7
- Chapter 3: The impact of APP scams 10
- Chapter 4: Prevention is better than cure 12
- Appendix 13



# Executive summary

APP (Authorised Push Payment) scams present a significant challenge that spans the financial services industry as well as many other sectors, including social media and telecommunications. In 2022 alone, APP fraud losses in the UK reached £485.2m.



In April 2023, Visa commissioned Mintel to conduct research among 2,000 UK respondents to understand the scale of APP scams and the impact they can have on victims. This report details the findings of the research and provides insight into the following:

**One in three consumers** surveyed have fallen victim to an APP scam, and it can happen to anyone, regardless of their demographic. The false sense of security created by an overconfidence in their ability to spot scams, makes APP scams a hidden, universal threat.

**The true scale of APP scams is unreported.** 25% of APP fraud cases are identified by the victim's bank, but in the remaining cases, barriers to reporting mean that 1 in 3 APP scams are unaccounted for in industry reporting figures.

**APP scams are continually evolving** and increasing in sophistication. Social media and instant messaging platforms are increasingly being used by scammers to target victims, alongside email and telephone. Empowered by technology, the authenticity of scams continues to improve, making it harder for consumers to spot them.

**Banks reimburse four in five recorded APP scam cases.** Despite the banks' best efforts to alert consumers of potential scams,

consumers still believe that banks are partially to blame for allowing APP scams to happen, contributing to the expectation that they should reimburse victims.

**The reporting and resolution experience influences the bank-customer relationship.** The resolution lead-time, frequency of communication and level of empathy shown to the victim can all impact how the victim feels about their bank. Even if reimbursed, 15% of victims leave their bank due to an APP scam.

**APP scams harm victims' personal and financial health.** One in three victims report that their mental health has suffered as a result of an APP scam, while many find that they have reduced confidence in money management.

**Consumers look to banks for prevention measures.** UK consumers believe that banks bear the primary responsibility for preventing APP scams from happening. Visa's suite of real-time payment analytics tools can create a coordinated, industry-wide view, helping banks to better identify APP scams.



**1 in 3**

consumers have fallen victim to an APP scam



**25%**

of APP fraud cases are identified by the victim's bank



**4 in 5**

APP scam victims are reimbursed



**15%**

of APP scam victims leave their bank



**1 in 3**

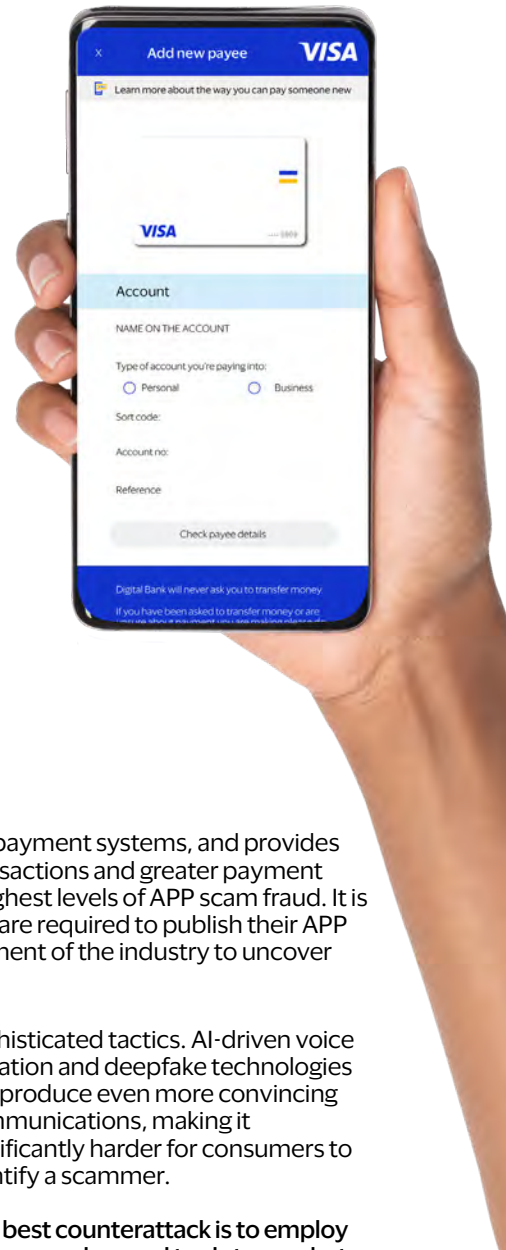
victims report that their mental health has suffered

# Market context

The UK's Faster Payment System, which was launched in 2008, facilitates the transfer of funds between bank accounts in real-time, at any time of the day or week, making it easier, faster, and more convenient for people to send and receive money. Over 70 other countries worldwide have now launched their own real-time payment systems. However, the growth of real-time payments has presented fraudsters with significant opportunities that they are capitalising on, at the expense of consumers, businesses, and the UK economy.

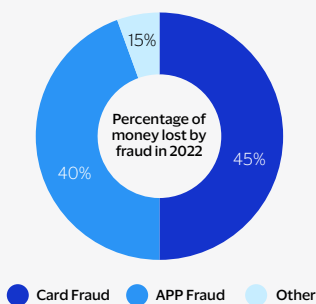
While traditional types of scams continue their downward trend, Authorised Push Payment (APP) scams, where customers are tricked into sending money to a fraudster posing as a genuine payee, are growing across the globe.

Markets with high and growing adoption of real-time payments, such as India, Brazil, and Australia, have seen the most significant increase in APP scam losses. In the US, while real-time payments currently form only a small part of the overall payment mix, APP scams grew 151% in 2022 and will likely continue to grow.



The latest figures from UK Finance show that £485.2 million was lost to APP scams in 2022<sup>1</sup>, meaning authorised fraud accounted for 40% of all UK fraud losses, gaining on the 45% contributed by card fraud.

**£485.2m**  
lost to APP scams in 2022



The UK has one of the most developed faster payment systems, and provides businesses and consumers with real-time transactions and greater payment flexibility. However, it does see some of the highest levels of APP scam fraud. It is also one of the very few markets where banks are required to publish their APP scam case numbers, highlighting the commitment of the industry to uncover and tackle APP scams.

While the UK's financial sector is working hard to tackle fraud, the scale and value of APP scams continue to grow, making it clear that there is more that needs to be done. The UK Government's new fraud prevention strategy will make victim reporting easier and commits to improving how law enforcement responds to fraud.

Fighting APP scams is no easy feat; we're up against an increasingly formidable opponent. With rapid technological advancements at their disposal, scammers are harnessing tools like AI to devise ever-more

sophisticated tactics. AI-driven voice imitation and deepfake technologies can produce even more convincing communications, making it significantly harder for consumers to identify a scammer.

**The best counterattack is to employ the same advanced tools to combat APP fraud scams. Just as scammers exploit AI and data analytics, the industry must harness these technologies for good. By refining its data-driven strategies, the industry can bolster its defences against these evolving threats.**

1. Over £1.2 Billion Stolen Through Fraud In 2022, With Nearly 80 Per Cent Of App Fraud Cases Starting Online

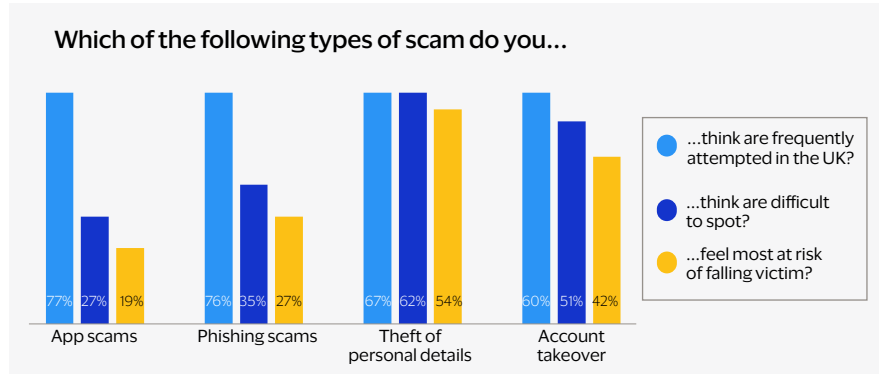
Mintel research commissioned by Visa Europe, conducted among UK Internet users aged 18 and above, between 28 April 2023 and 12 May 2023. See appendix for details and methodology.

# APP scams, a hidden threat

APP scams can pose a significant threat to consumers. But, this is not seen due to misconceptions around perceived risk, evolving tactics by scammers, and the psychological manipulation they employ.

## One in three consumers have fallen victim to an APP scam

While 77% of UK consumers recognise that APP scams are frequently attempted, a strong belief in their ability to detect them creates a false sense of security. One in three consumers have fallen victim to an APP scam, emphasising the dangers of complacency.



## Scammers exploit multiple channels

The increased adoption of digital communication channels, accelerated by COVID-19 lockdowns, has enabled scammers to leverage a wider variety of channels.

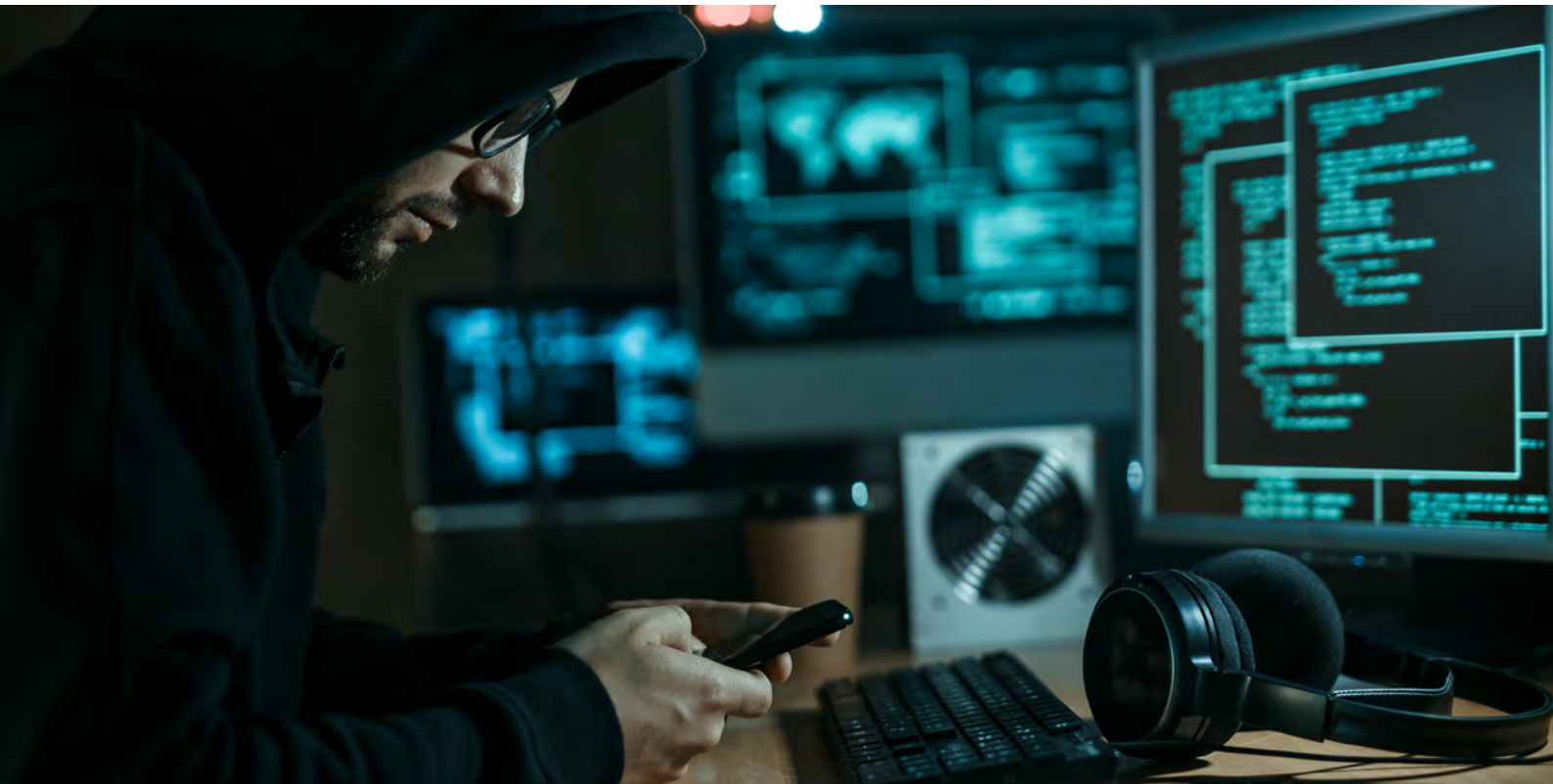
While large volumes of APP scams still originate via telephone and email, in the last five years, social media and other instant messaging services have increasingly been used to target victims.

Channel of initial communication used by scammer	<1 year ago	Change vs 5 years ago
Email	21%	+ 1 ppt
Social media direct messaging (e.g Instagram, TikTok)	21%	+ 17 ppt
Telephone	18%	-3 ppt
SMS text	15%	no change
Instant messaging services (e.g Whatsapp, Messenger)	10%	+6 ppt
Direct message through another type of app (e.g dating app)	4%	no change
Other communication channel	4%	-6 ppt



## Evolving technology increases scam effectiveness

Empowered by technology, scammers are making both their initial and ongoing communications more authentic, convincing, and detailed, increasing their chances of success.

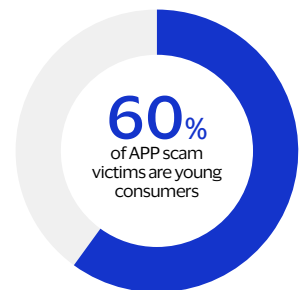


## Anyone can fall victim to an APP scam

Scammers exploit emotional vulnerabilities to create convincing narratives tailored to victims' circumstances.

Those facing significant life changes such as divorce or job loss are four times more likely to become victims of APP scams.

However, scammers successfully target consumers from all demographics and lifestyles, including younger consumers, who account for 60% of APP scam victims.



## **A** Education and collaboration **B** **C** is needed

Consumer education tools are already in circulation, with advice and guidance being provided by many in the industry, including networks, financial institutions, Action Fraud, and not-for-profits.

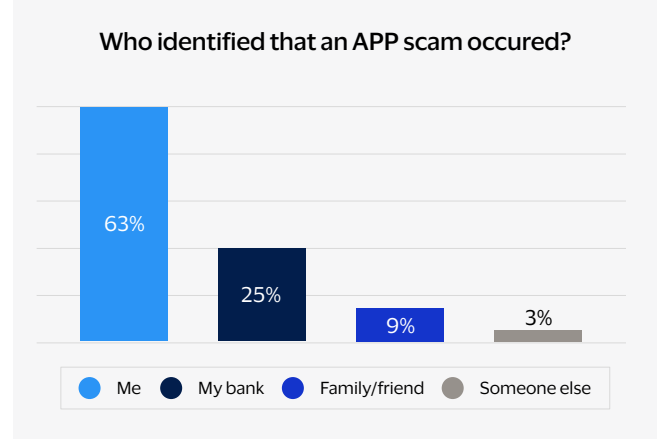
With two-thirds of UK consumers feeling the need to take steps to protect themselves from APP scams, a comprehensive approach involving financial institutions, law regulators, and consumer awareness is vital to rectify misconceptions and highlight the true prevalence and sophistication of these scams.



# Discovery and resolution

## 63% of victims are self-identified

In the vast majority of cases, it is the victim themselves, a friend, or a family member who realises that an APP scam has occurred. Just one in four are identified by banks, who then alert the victim.



Regardless of whether it's the victim or the bank that identifies the scam, victims undergo a series of intense emotions. The study found that shock, confusion, and panic quickly set in as victims recall warning signs and fear it is unlikely that an

authorised payment will be reimbursed, with humiliation found to be the dominant emotion. Despite having been tricked by a professional scammer, self-blame and self-criticism are common, as victims feel they should have been able to detect the scam.



**"I felt immediate shock and a heart-wrenching feeling."**  
- Male, 39, purchase scam.



**"I felt so foolish because it was me who wasn't quick to notice."**  
- Female, 35, Investment scam.



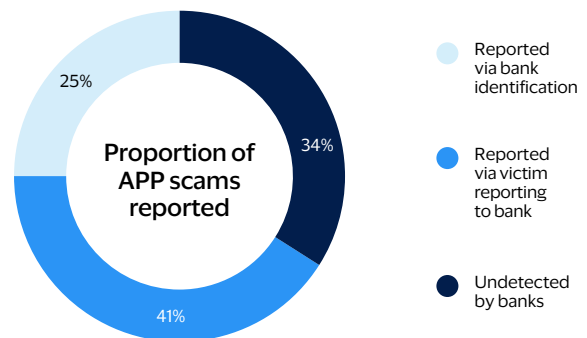
**"I am a gullible idiot and shouldn't have done that."**  
- Male, 19, Invoice scam.

## The true scale of APP scams is unreported

The 25% of APP scams that are identified by victims' banks are automatically captured and included in industry reporting figures, while the remaining 75% of self-identified victims are left to report the scam themselves.

Many of those self-identified victims do not report the scam to their bank, resulting in 34% of all APP scams going unknown to banks.

19% of all APP scams go completely unreported to any authority.



## Reasons for not reporting

When asked why they didn't report the scam, more than half of the victims said they didn't think they would get their money back, or that they didn't think anything could be done about it.

**One in five said they didn't report because they didn't know who to report it to, while others were put off by what they assumed would be a long or complicated process.**

Due to the nature of APP scams, victims often cite shame as a reason for not reporting, claiming that they didn't think their case would be taken seriously.



## Banks reimburse 4 in 5 APP scams

Despite their prevalence, a significant proportion of victims get their money back, with banks reimbursing 78% of APP scams they are aware of.

In the UK, banks are not legally obligated to reimburse victims of APP fraud, but many have signed up to the 2019 Contingent

Reimbursement Model Code, which commits them to taking steps to protect customers from APP scams, including reimbursement in some circumstances.

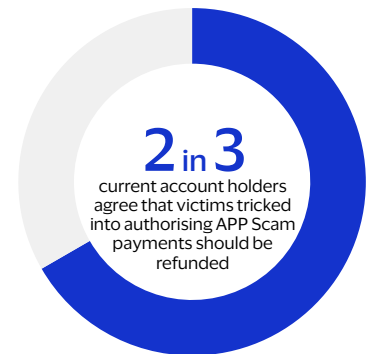
While a strong reimbursement rate is a positive outcome for victims, the cost of doing so for banks, is high.

## Reimbursement is an expectation

The general perception among consumers in the UK is that reimbursement shouldn't be optional. While there is an understanding that APP scams require authorisation and therefore victims are partially at fault, more than two-thirds of current account holders believe that victims should be reimbursed. Customers question why victims should be left out of pocket when they've been tricked by the psychological

manipulation techniques imposed on them by professional scammers.

Much of the expectation for banks to reimburse victims exists due to the belief that banks are partially to blame for allowing scams to happen in the first place. While half of APP scam victims accept sole responsibility for allowing the scam to happen, the other half say their bank should take some, if not all, of the responsibility.





## Consumers look to banks for prevention measures

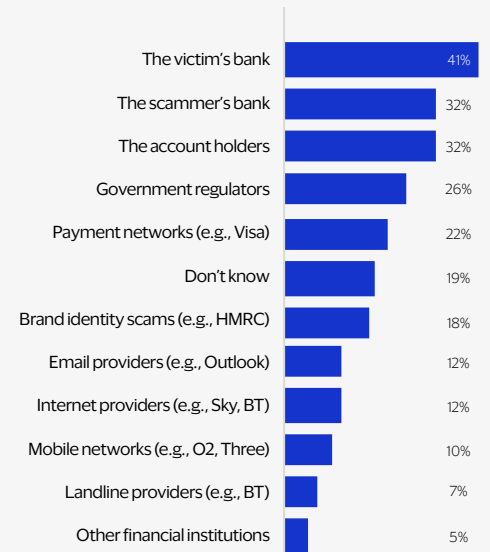
UK consumers believe that banks bear the primary responsibility for preventing APP scams from happening, more so than consumers themselves, government regulators, or payment networks.

Given upcoming changes in regulation that will make banks **liable** for reimbursement, banks must seek to proactively identify scams **before they occur** and prevent them from happening, in order to reduce financial losses for both themselves and victims.

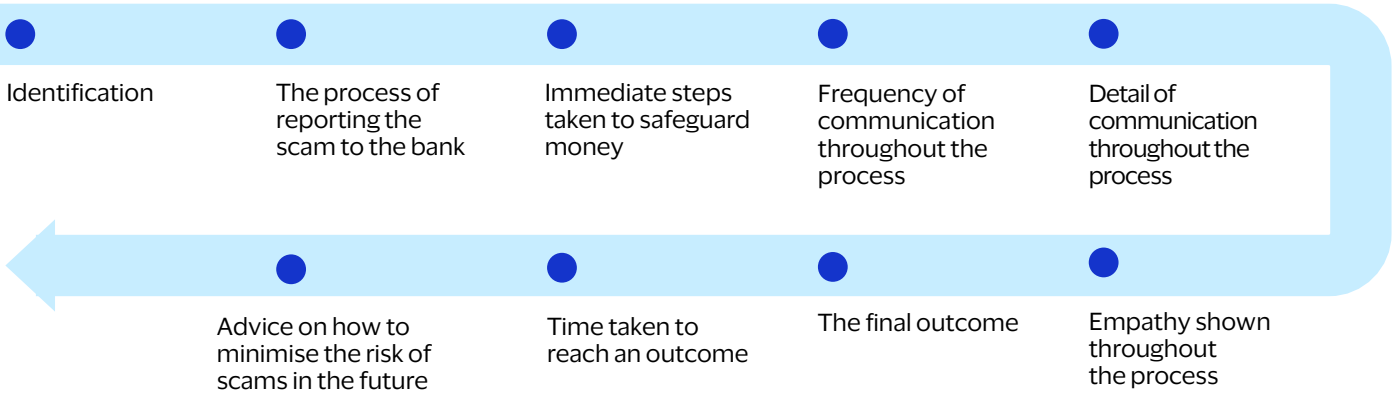
## Managing victim experience and satisfaction

Reimbursement isn't the only concern in APP scam resolution. The experience of the resolution process also impacts the victim's overall satisfaction with their bank and the ongoing bank-customer relationship.




Who do you think has the most responsibility to prevent APP Scams from occurring?  
Please select up to 5.



## The resolution process

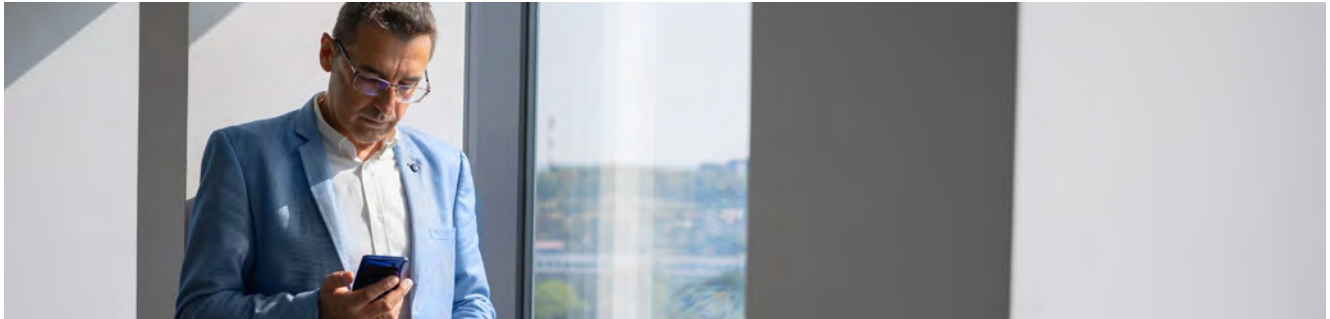


As part of this research, victims were asked how well their bank handled different aspects of the APP scam resolution process, which uncovered **the top three actions that banks can take to help improve overall victim satisfaction:**

-  The process of reporting the scam
-  The final outcome
-  The time taken to reach the final outcome

Failing to resolve APP scams quickly and efficiently can have a detrimental impact on how the victim perceives their bank. The resolution of APP scams demands resource, a cost that is set to increase as victim reporting and reimbursement expectations rise under new legislation.

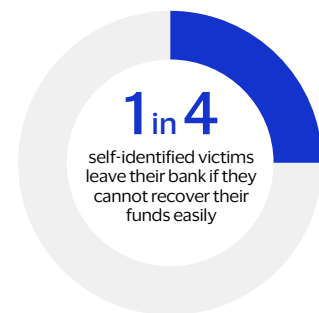
# The impact of APP scams



## 15% of surveyed APP scam victims leave their bank

The way a victim is supported through an APP scam influences the relationship they have with their bank. People view banks as secure custodians of their money, meaning fraud and lost funds can be deeply unsettling. A diminished

sense of security, reduction in trust and a perception of failed duty of care, particularly if victims are not reimbursed, can all influence the bank-customer relationship. In fact, 15% of surveyed UK APP scam victims left their bank as a direct result of an APP scam.



**Reimbursement will not always stop victims leaving**

Even victims who are reimbursed can lose trust in their bank. **51% of victims say that trust in their bank was affected because of the APP scam.**

## APP scams harm victims' personal and financial health

APP scams have a significant impact on various aspects of victims' wellbeing. Regardless of the outcome, victims tend to blame themselves. Feelings of guilt can impact victims' sense of self-worth, many report periods of isolation due to shame and embarrassment.

Where significant losses occur, APP scams can inflict both mental and physical health problems. Victims report periods of depression, anxiety, and loss of sleep.



**27%** of victims say the scam has had a detrimental impact on how they feel about themselves

**13%** of victims found that the APP scam damaged their personal relationships



"Lost £2500 which was hard to deal with. My mental health is now very bad. I can't face people now."



"I was shaking with anxiety. I feel quite vulnerable and an easy target."



"For a long time afterwards I could not sleep."

APP scams disrupt personal cash flows, often leaving victims struggling to pay bills, forcing them to reprioritise spending or borrow money from loved ones.



**Awful – had no money to pay any bills for 7 weeks. The bank was so unhelpful, had to borrow from my daughter.**



The consequences of APP scams extend to victims' future prospects. Unplanned overdrafts, damaged credit scores, and disrupted living situations are all impacts victims have felt as a result of an APP scam.

Under the new Consumer Duty rules that set higher standards of consumer protection within financial services, it will be critical for banks to consider the vulnerability of victims of scams and provide them with support when they need it.



**23%**

of victims said that the APP scam adversely impacted the amount of money they have available for day-to-day spending

## Reduced confidence in money management

While 58% of UK consumers surveyed said that they were confident in managing their finances, our research shows that falling victim to an APP scam can change money management habits. Those surveyed, who had been victims, grew sceptical of online payments and had reduced confidence in online banking. If victims start avoiding online channels, they will likely seek more costly alternatives.



**Made me more nervous about making payments or trusting anybody, even when family members are asking for money.**



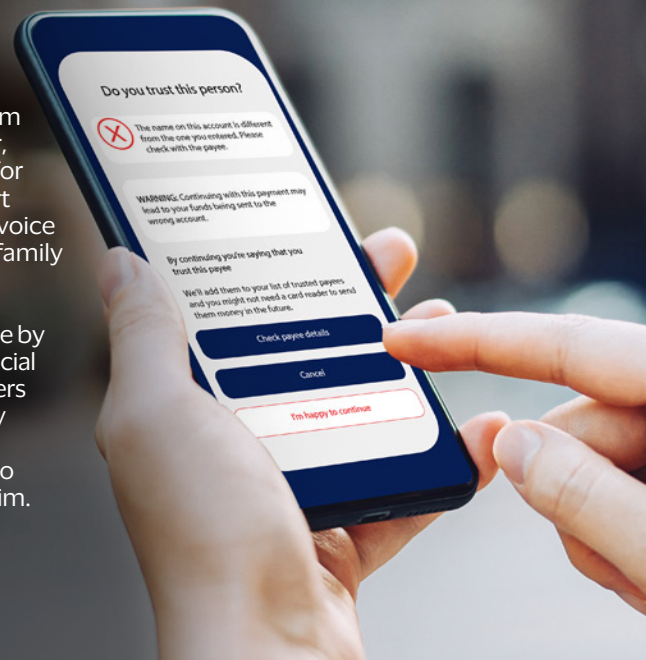
## APP scams will continue to evolve

Despite what they go through personally and financially, victims cite being more aware of the risks and how to spot the signs of an APP scam. Victims often become far more vigilant when assessing communications and cautious about making payment, helping to reduce the risk of falling victim again.

Unfortunately, however, as scammers continue to evolve their tactics and as scams become more sophisticated, it has become even harder for people to identify them.

An alarming example comes from America, where, earlier this year, the Federal Trade Commission for Consumer Advice issued an alert highlighting scammers using AI voice cloning technology to enhance family emergency scams.

By cloning the voice of a loved one by using audio or video clips from social media or online content, scammers convince victims they are a family member in need. The imitation is so realistic, that it is very difficult to identify and people easily fall victim.



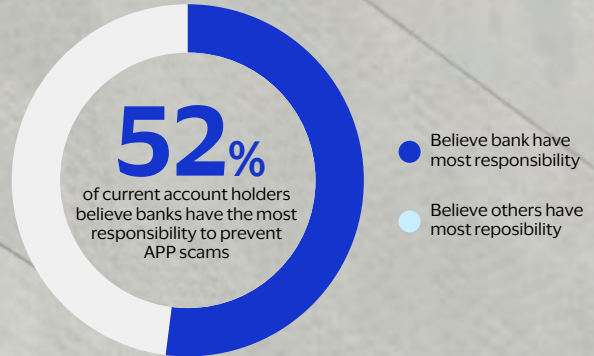
## Prevention is better than cure

### APP scams have detrimental effects on both victims and banks.

The potential loss of customers, reduced confidence in financial products, financial costs, and the impact on customer wellbeing highlights the importance of preventing these scams.

Although progress has been made throughout the industry, with initiatives such as delaying faster payments and verification of recipient names, the risk of APP scams remains high. The industry must continue to innovate to find solutions that unite financial institutions against these threats, allowing them to work together and leverage the wealth of data available, in order to stop scammers and protect consumers.

There is also a high expectation among UK consumers that banks should not only be able to prevent APP scams, but that they have the most responsibility to do so. 52% of current account holders believe banks have the most responsibility to prevent APP scams.



For more information or to learn how Visa can help with your fraud prevention strategy development, please contact [RTP@visa.com](mailto:RTP@visa.com).



# Appendix

## Methodology

Visa has collaborated with strategic insight partner, Mintel, to conduct research into the awareness, understanding and perception of APP scams among consumers in the UK as well as a detailed view of the victim experience.

To explore the objectives of the research, we used the following research methodology:

- Methodology: Online quantitative survey
- Market: UK
- Target audience: Internet users aged 18+, of which 300 were APP scam victims
- Sample size: 2,000
- Quotas: Demographic representation across the UK
- Survey length: 15 mins
- Fieldwork dates: 28th April 2023 - 12th May 2023

The survey first asked a number of questions to the general population about their personal situations,

financial behaviour and attitudes towards APP scams. A detailed section of the questionnaire identified victims of APP scams who were then asked a series of questions about their experience with APP scams.

It is important to note that the data in this report, including figures related to victim counts and losses, originates from self-reported victims of APP Scams. Some of these individuals may not have officially reported the scam to their bank or relevant financial authorities. Consequently, there might be discrepancies between the statistics presented here and industry reports, which typically rely on data from cases directly identified or reported to banks.



## Glossary

### Authorised Push Payment (APP) scam

APP scams are a type of fraud that happen when someone is tricked into sending money to a fraudster posing as a genuine payee. APP scams differ from other types of fraud, where criminals get access to accounts and steal money without the account holder's knowledge.

### Types of APP scam

#### Invoice and mandate scams:

Scammers intervene when a victim is trying to pay an invoice to a genuine payee and convince the victim to redirect the payment to an account they control.

**CEO scams:** Scammers impersonate chief executive officers (CEOs) or other high-ranking officials of organisations then try to convince victims to make an urgent payment to the scammer's account.

**Impersonation scam - police or organisations:** In this scam, a criminal gets in touch and pretends to be

from the police or the victim's bank and convince their victim to make a payment to an account they control.

**Impersonation scams - family or friends:** Fraudsters pretend to be a family member or friend and typically will make up a story about needing help or being in trouble and will ask the victim to make a bank transfer.

**Purchase scam:** Scammers convince you to pay in advance for goods or services that are never received.

**Investment scam:** A criminal convinces you to move your money

to a fund that doesn't exist or to pay for a fake investment, usually promising a high return.

**Romance scam:** Scammers start a relationship using fake dating or social media profiles and will develop it over a long period of time. When they believe they have the victim's trust, they will then claim to have a problem and ask for money to help.

**Advance fee scam:** Scammers convince victims to pay a fee that they claim will result in the release of a much larger payment or high value goods which never materialise.

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or "best practices" may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.