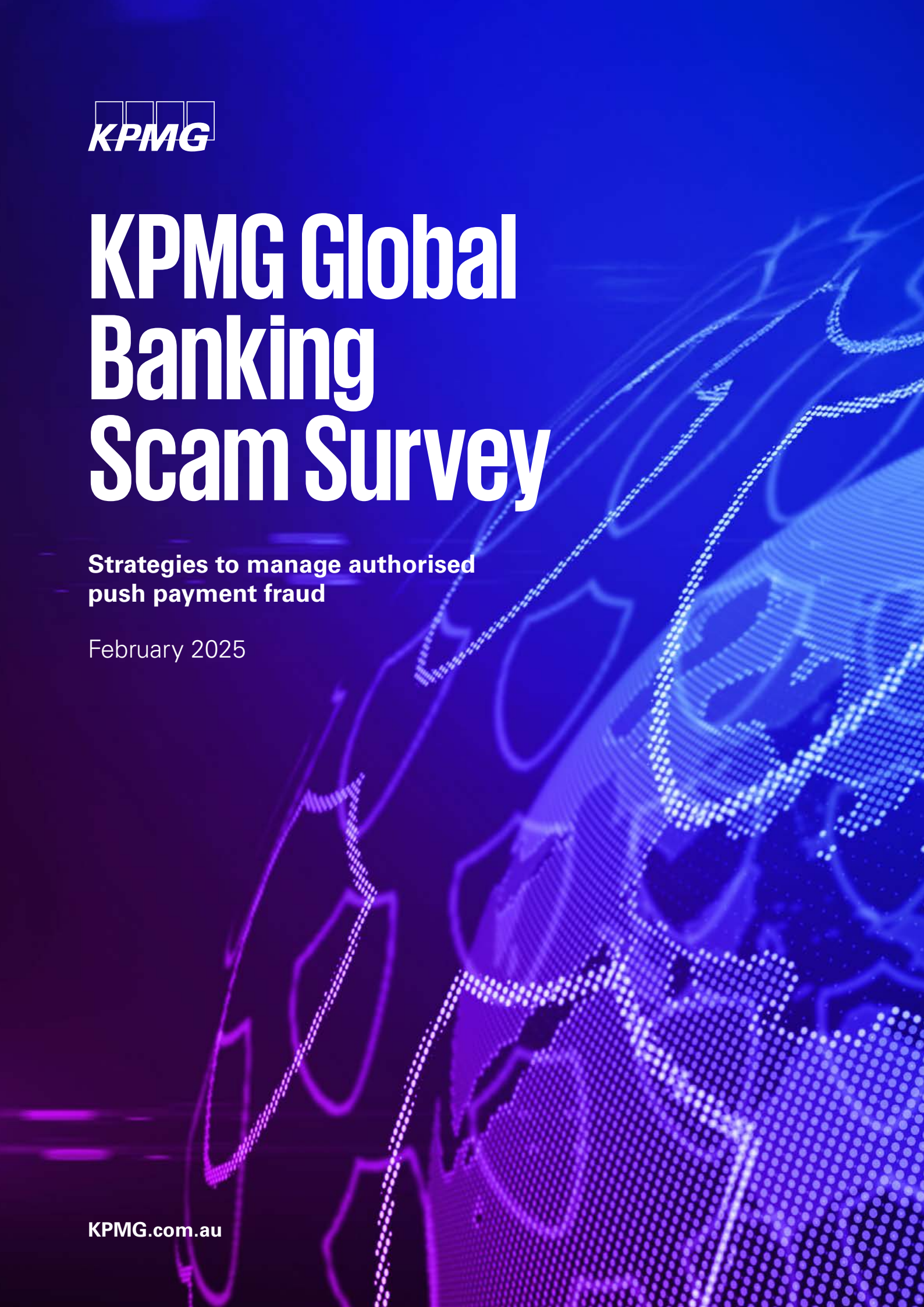


KPMG Global Banking Scam Survey

Strategies to manage authorised push payment fraud

February 2025

KPMG.com.au

Foreword

Authorised push payment (APP) scams are global, transcend borders and affect all jurisdictions. The interconnected global economy and the ease with which information and money can be transferred across borders means one instance of an APP fraud can affect multiple financial institutions across multiple countries. Global scam losses are estimated in the billions each year.

APP scammers trick victims into making payments to accounts that belong to fraudsters. These scams often involve fraudsters impersonating a trusted entity, such as a bank, service provider or government agency, and using false pretences to convince the victim to authorise payments. The victim is led to believe they're making a legitimate transaction, when in fact they are sending money directly to fraudsters.

Banks and financial institutions are often seen as the 'gatekeepers' for consumer funds within the complex global ecosystem. In the context of APP scams, this ecosystem includes governments, regulators, telecommunications companies, technology and social media companies, cryptocurrency exchanges, law enforcement and consumers themselves.

KPMG's Global Banking APP Scam Survey encompasses the views of 48 banks in 16 countries and 5 continents to identify trends and best practices that enable these institutions to protect consumers. The survey data was collected through interviews with professionals in fraud and scam prevention. We sought to obtain a variety of views that include large multinationals, digital neobanks and mutuals/building societies.

We hope the insights provided in this survey will encourage organisations in all sectors to reassess their scam prevention strategies and consider how they can enhance them to bolster global fraud protection efforts.

Martin Dougall
Partner in Charge – Forensic, KPMG Australia
Global Forensic Network & Solutions Leader

KPMG's APP Scams Global Banking Survey – coverage

48 BANKS

16 COUNTRIES

5 CONTINENTS

Americas	
Canada	5
USA	3

APAC	
Australia	5
Singapore	4

EMEA	
Germany	1
Greece	3
Italy	1
Netherlands	3
Norway	3
Portugal	2
Spain	2
South Africa	3
Sweden	3
Switzerland	1
Türkiye	2
UK	7

Americas
APAC
EMEA

Contents

Key insights

Trends

Global patterns are consistent for APP scams with e-commerce scams the largest by volume, and investment scams the largest by financial impact.

Strategy, policy and governance

Specialist teams and committees regularly review scam control measures within their organisations, sometimes daily. These teams consider global insights, trend analysis and customer feedback.

Prevention

Pausing and blocking transactions were rated as the most effective method of prevention. Confirmation of payee was thought to be less effective but an expected minimum standard to combat basic scams.

Detection

Sharing data with law enforcement, a consortium of peers or industry bodies was rated as the most effective measure of scam detection.

Response

Although 45% of banks surveyed will off-board repeat scam victims, this is considered a last resort decision taken by senior committees and usually only where there is first-party fraud.

Technology

Almost two in every five respondents don't have a technology stack with orchestration layers integrating a multitude of data sources into a single system, but they see this as a priority for their scam reduction efforts.

Complaints

Scam-related customer complaints increased for 60% of respondents. The most frequent complaints were dissatisfaction with reimbursement decisions, frustration with friction in transactions, the speed of resolution and feeling the bank could do more to protect the consumer.

Customer education

It was broadly agreed that education needed to be continuous and across multiple platforms. Scam awareness campaigns were felt to only be effective for a short time.

Survey results

1. Scam trends

These results provide a global snapshot of the current scam landscape affecting banks. Our data shows some of the most frequent frauds aren't necessarily new typologies and that the pattern and trends of APP scams are consistent for our participants around the world.

E-commerce and purchase scams

Fraudsters exploit online marketplaces to trick victims into making purchases that are never delivered. These scams are typically for products that are high in volume but low in value, although some banks reported larger value cases related to cars. This type of scam tends to spike around major entertainment events, creating demand for tickets and leading scammers to sell fake tickets online.

Investment scams

These scams often involve fraudulent investment opportunities where the underlying asset doesn't exist, or legitimate opportunities where consumer funds aren't invested as promised and the scammers make off with the funds. These scams frequently promise high returns and have a significant impact on consumers as they often involve large sums of money, sometimes even their life savings. Current examples include:

- **Fake deposit scams:** The fraudulent investment is presented as a bond or long-term deposit in a well-known company.
- **Boiler room scams:** Fraudsters use high-pressure selling techniques to persuade consumers to purchase securities at inflated prices.
- **Fake cryptocurrency investments:** Fraudsters create false cryptocurrency products, exchanges, websites or apps to encourage 'investment' from consumers who never see their money again.

Sophisticated impersonation scams

Impersonation scams continue to evolve and are becoming more sophisticated, with scammers leveraging social networks, emails and phone calls to trick victims into sharing sensitive information or transferring funds. These scams often involve manipulating legitimate documents, making subtle changes to names or email addresses to enable the fraud.

- **CEO scams:** In these scams, fraudsters impersonate high-ranking executives, often the CEO, to trick employees, customers or vendors into transferring money or sensitive data. These scams are typically conducted via email and often create a sense of urgency. Recent iterations have seen fraudsters make targeted attacks on junior staff and new hires using augmented AI and

tracking professional updates to job profiles on social networks. CEO fraud attacks occur less frequently than other scams but they often result in significant financial or reputational losses.

- **Impersonating bank employees:** This involves fraudsters impersonating bank staff to convince victims to transfer funds to an account that the scammer controls. This increasingly complex and professional 'helpdesk fraud' often involves the charade of transferring calls to other departments or providing fake reference numbers. There have been instances where genuine bank fraud teams identified high-risk transactions and contacted surprised customers who had executed the transaction under the instructions of fraudsters posing as bank fraud teams.
- **Workplace impersonations:** These scams target human resources and information technology (IT) teams, with victims receiving QR codes or malicious links which give the fraudsters access to funds or personal information.
- **Impersonating people of authority:** These scams involve impersonating authorities such as government officials or police officers. Scandinavia has experienced a worrying trend of physical meetings occurring between victims and these fake officials.
- **Tech support scams:** These scams involve impersonating IT or point of sale technical support to gain access to a customer's computer and personal information. They're also known as remote access scams.
- **Impersonating accountants:** In these scams, fraudsters impersonate accountants to provide fake tax returns or financial advice to their targets.
- **All the Ishings:** These scams involve sending deceptive emails (phishing), QR codes (quishing), text messages (smishing) or phone calls (vishing) claiming to be from a trusted company or a family member. They all aim to trick victims into revealing personal information, one-time passwords, downloading malware or making payments.

Romance scams

These APP scams involve fake profiles on dating sites, apps or social media platforms to lure potential victims into online relationships.

Scammers often use stolen photos to create attractive and convincing personas that 'live' in a different location to their victims.

They can spend months building trust within their targets, often communicating via chat, email or phone calls. Eventually, they ask for money under the guise of personal hardship, family emergency or the desire to visit the victim in person. In addition to financial losses, romance scams have a significant psychological and emotional impact on the victim.

Advanced fee and payment scams

These scams involve victims paying upfront fees for services or goods that don't exist. They include:

- **Fake travel companies** who advertise cheap holidays and request upfront payment whilst also stealing sensitive information like passport details.
- **Lottery scams** where victims are asked to pay a fee to collect their winnings.
- **Job scams** with fraudulent job offers which often require victims to pay upfront fees or share sensitive information.

Business email compromise

Also known as BEC scams, this approach compromises legitimate business email accounts through social engineering or cyber intrusion to make unauthorised fund transfers. These scams are known for disguising fraudulent payments as legitimate vendor invoices. One respondent reported an increase of BEC attempts which relied solely on customer manipulation to change details or redirect funds without any form of digital involvement.

Blurring and hybrid scams

These scams combine elements of different fraud and scam types and include:

- **Romance baiting:** Victims of romance scams are gradually lured into making increasing contributions to an investment scheme. Once the investment reaches a significant size, the fraudster absconds with the funds. This practice is also known as butchering or slaughtering.
- **Recovery scams:** When the victim realises they've been scammed, recovery firms offer their services to find the lost money, but payment must be made in advance. This recovery firm is part of the scam and the victim loses even more money.

Deepfakes

A deepfake uses technology to create images of fake videos, audio or words that are convincingly real. The survey revealed a consensus among participants that the application of deepfakes and generative AI (Gen AI) in APP scams wasn't currently prevalent, but it was acknowledged as a potential future risk.

Many banks report minimal encounters with deepfake scams or AI-generated frauds. Most successful fraudulent activities are still conducted using simple, low-tech methods.

Instances where banks have encountered deepfakes include:

- Using Gen AI to falsify documents including counterfeit passports that are used in the identity verification and know your customer (KYC) processes.
- Using Gen AI to generate convincing scam emails and messages, including translating emails into different languages to adapt them to targets all over the world.
- Using deepfake-produced personas for romance scams.
- Using Gen AI to produce fraudulent bank impersonation websites.

Banks saw deepfakes being more widely used directly against customers rather than themselves. For example, investment scams on social media featuring deepfakes of prominent celebrities and public figures.

Banks acknowledge that detecting deepfakes and AI-generated scams is challenging, particularly as they are not yet common practice. Some banks are investing in third-party software to detect these.

Despite the current low prevalence, there's a general expectation that the use of deepfakes and AI in scams will increase. Banks are cognisant of this potential risk and are monitoring developments. One bank noted the risk of impersonation of high-profile customers and is planning to train staff to ask questions to assess if the customer is genuine.

Targets

The survey revealed that scammers most frequently target retail and business bank accounts, and retail customers are their primary victims.

Most participants noted that scams often target older customers, although this depends on the fraudsters' modus operandi.

Investment and tech support scams target an older demographic, who are also believed to suffer the greatest losses. Younger demographics are more often the target of e-commerce and cryptocurrency scams.

Digital platforms, particularly internet and mobile banking, were frequently mentioned as the channels through which most scams occur.

Me-to-me payments

This is when a customer transfers funds between their own accounts with different banks. The banks initiating these transactions have expressed concerns about their ability to identify whether a customer intends to use the transferred funds for unauthorised scam payments.

2. Governance

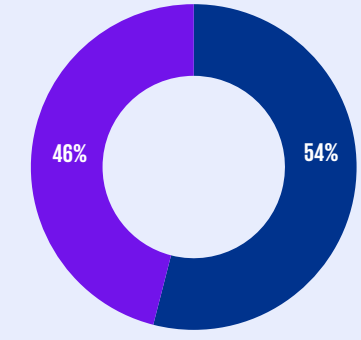
Scam strategies

Our research indicates the industry is divided when it comes to using distinct bank-wide scams protection strategies and policies.

More than half of the banks surveyed already have or are working towards a dedicated scams policy, assigning clear governance with board endorsement and designated responsibilities for oversight.

The other 46% of respondents direct their efforts through integrated fraud prevention frameworks with scam strategies commonly embedded within broader fraud prevention initiatives, providing a unified approach.

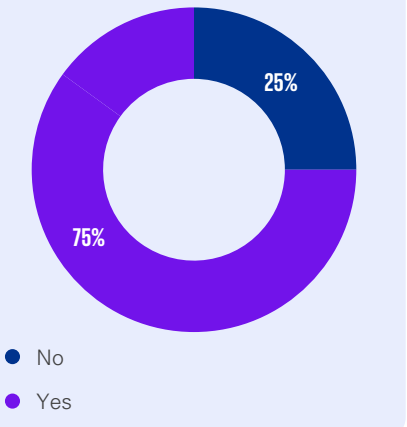
Do banks have a bank-wide scams policy, distinct from fraud?



Risk assessments

We asked banks if they performed a risk assessment for APP scams. Most confirmed they do, though some are included in product or fraud risk assessments.

Have banks performed a risk assessment to identify effectiveness of controls to mitigate APP scams?



Adaptability

We asked how banks make sure their APP scam strategy and approach is responsive to new scam typologies, banking products and delivery channels. The responses featured several common themes:

- **Regular reviews** (29%): These banks conduct frequent (daily, weekly or monthly) reviews of their fraud control measures, incorporating global insights and customer feedback.
- **Collaboration and information sharing** (38%): Many banks emphasised the importance of sharing information on new scam typologies both internally amongst their own teams as well as externally with industry groups, law enforcement and other banks.
- **Data-driven approaches** (15%): Data analytics and machine learning was a recurring theme, as banks use these technologies to quickly identify and respond to emerging scam trends.
- **Specialised teams and committees** (19%): Banks often have dedicated fraud risk committees or specialised teams that meet regularly to evaluate current fraud cases, strategise and implement responsive actions.

Other approaches included:

- **Root cause analysis:** It was a common practice for respondents to invest time and resources to understand how scams occur and to develop appropriate countermeasures.
- **Scenario-based strategies:** Some banks use dynamic, scenario-based strategies that are regularly evaluated and updated to adapt to new types of scams.

Customer reimbursement

We found 87% of the banks stated their policies and standards included guidance on customer reimbursement when fraud occurs.

We asked how they determined when to provide full, partial or no reimbursement and their responses had two main themes.

The survey found that:

Most banks with a consistent approach to reimbursement have organisation-wide frameworks and decision trees which incorporate goodwill gestures and regulatory drivers.

Of the global banks that responded, only 23% have a universal policy on APP scam reimbursements. This highlights the challenges and diversity of regulatory landscapes.

For those with a case-by-case approach to evaluating reimbursements, one bank had empowered its operations team to refund smaller amounts with larger amounts going to a committee for approval.

Regulatory compliance

Some participants anchored their reimbursement practices in laws and regulations. These included the UK's Contingent Reimbursement Model Code (CRM Code) or voluntary agreements such as the Netherlands' *Criteria for awarding compensation for loss arising from bank help desk scams ('spoofing').*

Case-by-case evaluation

Other participants took a more flexible approach, analysing each case individually. They applied criteria including whether any warnings were provided, customer vulnerability, if it was a first-time offence, client behaviour and operational slip-ups.

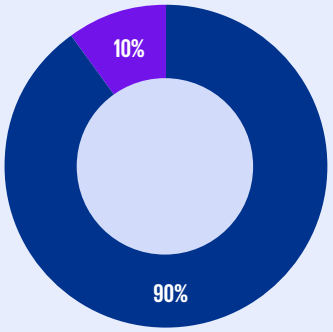
Management reporting

An overwhelming majority of banks surveyed, 90%, acknowledge the importance of specifically tracking customer scam losses separately to fraud losses. This was often seen in the form of distinct line items in reports or as topics of focus in committee meetings.

Of those 90%, the majority include operating performance and operating cost as part of management information.

A 10% minority has yet to distinguish scam losses in their management reporting.

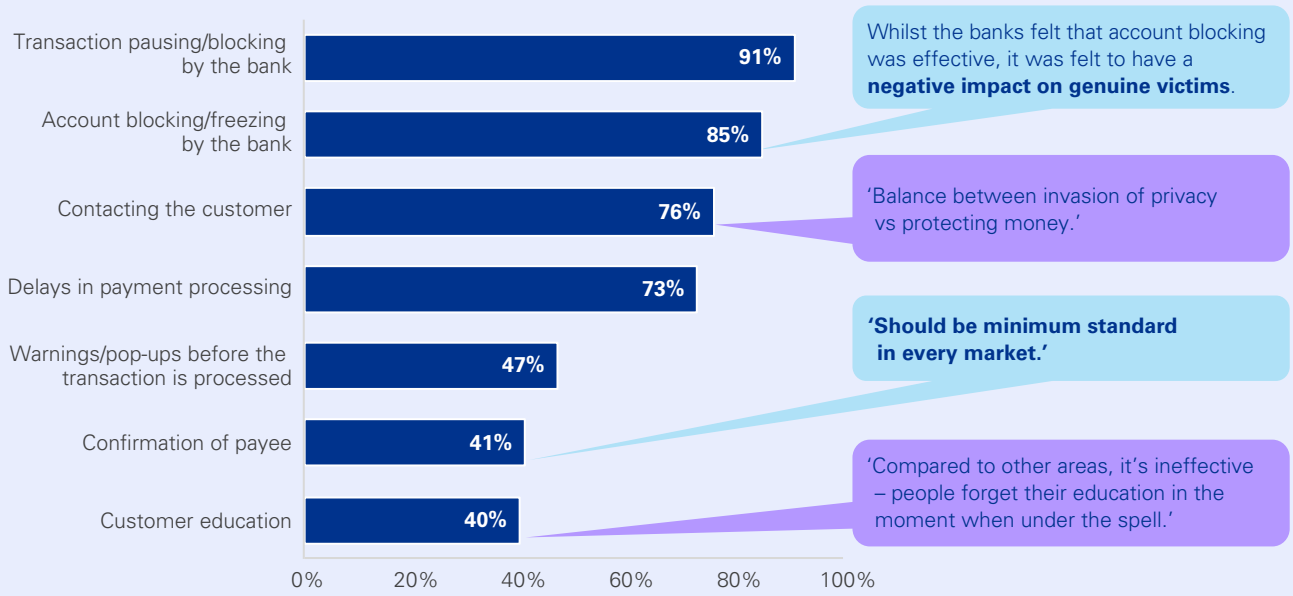
Do banks track scam losses distinctly from fraud losses?



3. Prevention

Prevention measures are the strategies and controls implemented to protect individuals and organisations from scams occurring. Survey participants were asked to assess the effectiveness of each scam prevention measure if they had it in place.

Scam prevention methods



Pausing and blocking transactions

Banks can pause transactions, temporarily stopping potentially fraudulent activity and restricting all account transactions, while they investigate suspicious behaviour.

A significant 91% of respondents rated transaction pausing or blocking as an effective scam reduction measure. The banks will block based on red flags and risk scoring which examines factors such as source, destination of funds and tenure of the customer.

'Effective but mule accounts are churned very quickly these days, so there is a narrow window of opportunity.'

Freezing and blocking accounts

When a bank restricts access to an account due to suspicious activity, the account holder can't withdraw funds, make transfers or any transactions until it's released.

'We have persistent monitoring so we can be quick to freeze the accounts where an issue arises.'

Whilst 85% of the banks felt that account blocking was effective, it was seen to have a negative impact on genuine victims. But it was felt to be an effective approach for managing mule accounts (accounts used to transfer or launder money obtained illegally).

Disabling these accounts disrupts the financial networks scammers rely on, cutting off a critical pathway for moving illicit funds. Many banks have implemented daily monitoring systems, cross-referencing known mule accounts against industry databases.

Contacting the customer

This involves banks communicating directly with customers via phone, email or text message to verify transactions and discuss potential risks. It serves as a direct method of fraud prevention and customer engagement.

'This is a balance between invasion of privacy and protecting money.'

Contacting customers to verify suspicious transactions was a highly rated measure, with 76% of respondents viewing it as effective. Most banks use in-app messages as well as direct phone calls for this contact. This was seen as important so staff could have effective conversations with customers to convince them of the potential risk of processing a suspicious transaction.

Delaying payments

This measure involves intentionally slowing the process of payment clearance to ensure adequate time to verify the legitimacy of the transaction. This reduces the likelihood of a scam's success.

Our results show 73% of respondents found delaying payments that triggered specific rules useful, as it provided time to investigate and speak to customers, if necessary. One bank moved from delaying such payments to outright declining them. These delays, ranging from 2 to 72 hours, were seen as helpful in high-risk scenarios and offered a valuable review period.

'Really effective when done well but very operationally intensive.'

Warnings and pop-ups

Banking websites and apps can show alerts or messages during online transactions, advising customers to confirm the legitimacy of a transaction before it's completed.

'Message fatigue has set in.'

Just 47% of respondents viewed this as an effective anti-scam measure. The banks state customers often become desensitised to generic warning messages, which reduces their impact. A more effective approach was felt to be targeted warnings at critical moments in the payment process which are connected to real-time risk scoring and include customer contact.

'Need to focus on targeted messaging with meaningful messages at the right time.'

Confirming the payee

This security feature seeks to confirm the customer-provided payee details match those in the bank system. This helps prevent misdirected payments and fraud, ensuring funds are sent to the correct recipient.

'Should be the minimum standard in every market.'

Just 41% of respondents see this as an effective measure. Many note that it provides a level of reassurance, improves customer experience and helps when customers make genuine mistakes. However, banks felt its effectiveness in scams prevention was limited, as fraudsters often sidestep this protection and coach victims to ignore it. That said, banks with this in place said that they wouldn't remove it as it still prevents immature scams.

Customer education

Banks inform and empower consumers to recognise, avoid and report fraudulent activities.

Customer education garnered a mixed response. Banks felt it was hard to measure its effectiveness. They reported education at multiple interaction points, including in-payment education (such as warnings and pop-ups) with real-time notifications during online transactions, at the 'moment that it matters' was the most effective.

'Compared to other areas, it's ineffective – people forget their education in the moment when under the spell.'

Other initiatives

'We have additional controls such as cooling periods for adding new payees, changing of addresses etc. The cooling period is 12 hours. It significantly slows down the actions of scammers, as well as preventing complete account takeover because of how long the process takes.'

'We have introduced analytics to detect employee involvement in scams under duress.'

'Savings account lock which prevents gaining access within 24 hours after unlocking.'

Two major Australian banks have tightened cryptocurrency policies, with one implementing a $10,000 monthly limit on crypto purchases and another blocking payments to certain high-risk platforms.

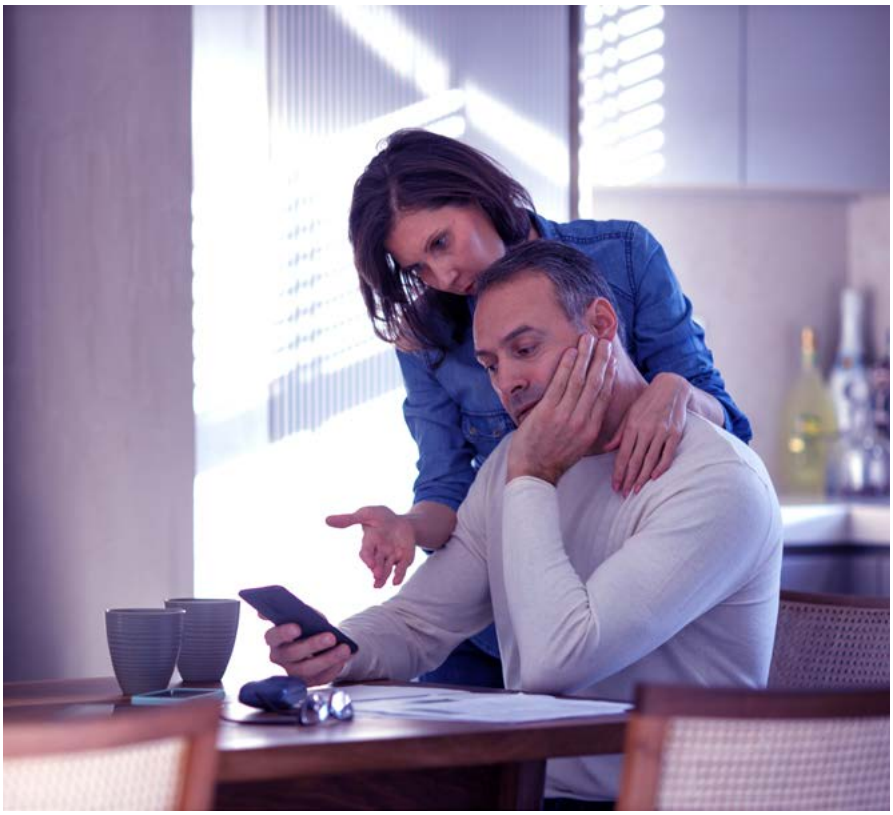
'Taking down fake bank websites and phone numbers impersonating the bank's helpdesk.'

Vulnerable customers

A significant 81% of surveyed banks attempt to identify customers at risk of scams. Some use regulator definitions, like those from the UK's Financial Conduct Authority. They understand vulnerability can stem from situations like illness, bereavement or major purchases, as well as more traditional variables such as age, health and financial resilience.

Some of the initiatives to protect vulnerable customers include:

- using customised monitoring rules, including smaller transfer limits for specific customer segments
- using machine learning to identify vulnerable customers, including assessing likelihood of fraud and the impact
- identifying recent scam victims in core banking systems
- providing tailored training to bank staff
- introducing additional approval processes for transactions, such as coming into branch
- using targeted education, such as information sessions for cohorts or speaking directly to customers about the risks.

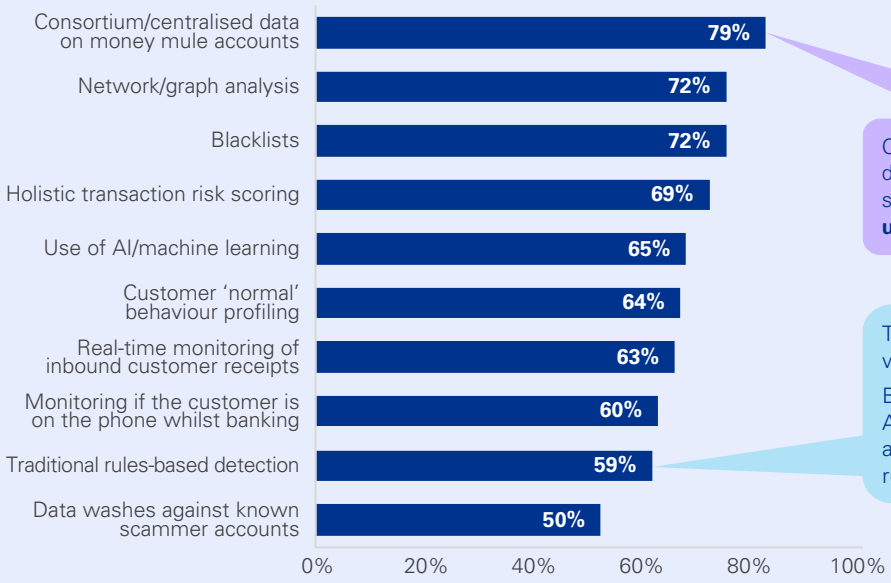


'We have a team that recognises vulnerability in monitoring activity and will speak to the customer if required. We have alerts in place to spot if customers are domestic violence or abuse victims.'

4. Detection

Detection measures are the strategies and processes implemented to identify fraudulent activities. Survey participants were asked to assess the effectiveness of each scam detection measure if they had it in place.

Detection methods



Countries without consortium/centralised data on money mule accounts, or with siloed approaches said **this was urgently required**.

Transaction rules-based detection was noted to be not useful in silo.

Banks also found that the use of AI/machine learning was effective as they used it to enhance their rule-based detection.

Data analysis and sharing

Banks and financial institutions hold data about their customers which can be analysed to detect potentially fraudulent activity. This analysis can occur within the organisation and the data on suspicious individuals or transactions can be shared with other banks and regulators to generate even deeper insights.

- **Consortium data** is information on individuals and transactions that's shared between different institutions. It can enhance scam detection by providing a richer dataset to enable recognition of fraud patterns and known bad actors.

  Banks that don't share data, or with siloed approaches, said the measure was urgently required and should be the responsibility of a government agency to implement and govern. Those with centralised data, either in a consortium or from government agencies such as the police, rate it as effective in preventing scams.

- **Network and graph analysis** makes connections between individuals and entities.

  Some participants said this helped fraud investigation teams to see the bigger picture, especially with mules. They feel this approach would work better when organisations collaborate and share information to increase the likelihood of matches.

- **Blacklisting** is the process of adding parties, including individuals or groups, to a list of known fraudsters on core banking systems.

  Banks find this effective when they could receive information from other sources like government agencies and consortiums. Some banks are using lists from local financial authorities to prevent investment fraud. Whitelists were also helpful, for example where customers are paying bills for friends or family members.

- **Holistic transaction** risk scoring rates transactions based on predefined factors such as geolocation, transaction patterns or values.

  Banks felt this was useful when combined with other initiatives, such as machine learning or behavioural biometrics.

- **Data washing** is the process where institutions regularly check customer transaction data against databases of known scammer accounts.

  Data washes against known scammer accounts, using internal and external blacklists was felt to be effective by 50% of our participants. It's effective in identifying relationships within fraud networks, but banks say it falls short when dealing with mule accounts without a previous fraud record. Most respondents indicated enhanced industry collaboration would improve the effectiveness of data washing.

'Effective – especially when network relationships are identified.'

AI and machine learning

AI and machine learning are increasingly being used alongside other fraud detection methods to improve fraud detection outcomes.

Banks rating this as effective referenced they used this to enhance their rule-based detection.

Monitoring customer behaviour

Core banking systems have the sophistication to proactively monitor customer behaviour for potentially fraudulent activity in their accounts or their activities.

More than half of our respondents (64%) said analysing **historical customer data to identify 'normal' patterns of behaviour** is effective in flagging abnormal transactions. One bank commented this is effective in reducing the rate of false positives (legitimate transactions that are erroneously flagged as fraudulent).

We found 63% of the responding institutions who **actively monitor incoming transactions** to customers' accounts in real time rated it as effective. They monitor to detect unusual activity or unauthorised deposits that may signal fraudulent or money mule activity. Its effectiveness depends on the maturity of the institution's implementation.

Some banks **monitor customers to understand if they're communicating with a third party** while using online or mobile banking. And 60% of our respondents with this in place rated this as an effective fraud prevention measure. Many banks were in the process of implementing this technology so couldn't yet comment on its efficacy.

And finally, a more **traditional rules-based approach** to detecting fraudulent transactions was rated effective by 59% of participants. These rules flagged transactions based on attributes such as geolocation, transaction patterns or their value. Some banks applied these rules to both inbound and outbound transactions. Some commented this approach wasn't effective alone, and banks needed to consider multiple factors.

'Effective, but not unless used in combination with other detection methods.'

5. Fraud responses

We asked banks about the structure and responsibilities of their fraud operations teams and how they investigated and resolved scam alerts.

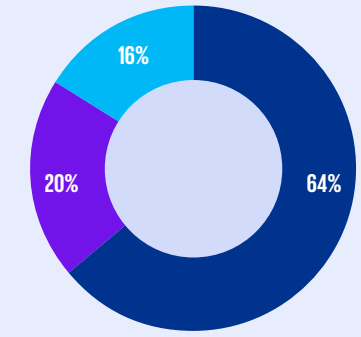
Scam operations team structure

Most banks reported a unified approach with scam operations functions sitting within fraud operations teams. Rather than having a standalone team, scam responses are managed within the broader umbrella of fraud prevention and response.

A minority, however, have carved out a niche for scam operations within specific departments, focusing on areas like digital payments and online banking.

Scam strategies

Do you have a separate scam operations team distinct from your fraud ops team?



Scam operations responsibilities

For banks with a dedicated scam operations team or specialised units within fraud teams, their responsibilities include:

- **Case management:** Reviewing scam cases, adhering to regulatory standards and determining the customer care pathway in more complex situations.
- **Investigations:** Probing alerts and suspected mule accounts.
- **Customer communication:** Some banks have 'break the spell' teams, which are specialised groups dedicated to helping customers recognise and resist the manipulative tactics, or the 'spell', used in scams. Some also act as a direct point of contact for the victim.
- **Asset tracing:** Tracing and recovering customer funds.
- **Claims:** Making claims decisions in scams cases. The complex cases can be referred to high-level forums.
- **Trend spotting:** Identifying trends and new typologies to inform educational material or warnings for customers to prevent future scams.

Fraud operations training

The survey responses illustrate the different training approaches that financial institutions employ when handling APP scam alerts.

- **Specific process training:** Some banks base their training on decision trees and have specific modules on how to manage potential scam victims.
- **Customer interaction and soft skills:** Teams are trained on effective listening and the judgement required to assess nuanced cases and have persuasive conversations to convince customers of the potential risks. Teams are also trained to deal with irate or defensive customers.
- **Scam typologies:** Banks makes sure that case staff are educated in current scam typologies so they can inform customers.

'Customer experience is important and includes helping the customer navigate the emotional trauma experienced. The scams team have to wear a fraud hat as well as have empathy for the victim.'

Fraud operations automated decisioning

Just over half of the banks, 56%, use automated rules to delay or freeze transactions or accounts. The banks generally don't use automated decisioning for reimbursements.

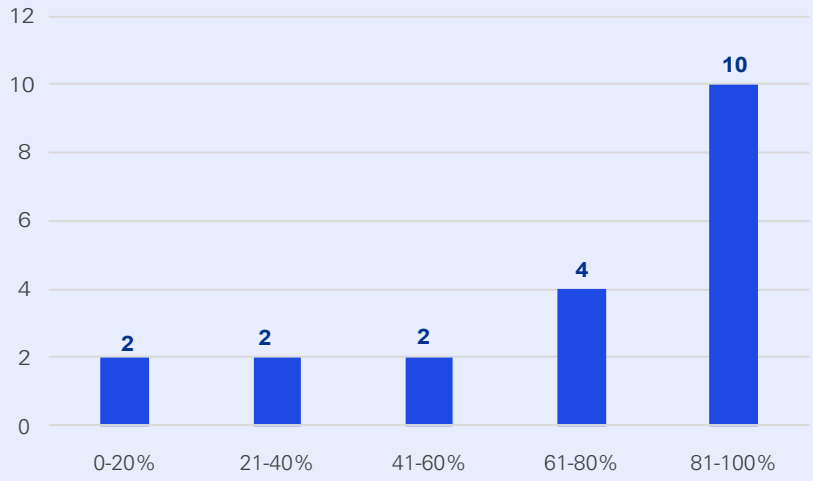
'Some areas need to be human-to-human.'

False positives

False positives are legitimate transactions that are incorrectly flagged as fraudulent. Just 42% of participating banks provided this data point. Of those respondents, the false positive rates were significantly high. This illustrates the challenge of identifying fraudulent APP scam transactions when by definition it is the customer themselves doing the transaction, so device checks as used on other fraud types provide no assistance. In addition, fraudsters are aware of bank controls and will modify the approach to seek payment amounts that will not trigger detection systems.

What is the false positive rate you are seeing for scam alerts?

This information was not tracked/available for 58% of the banks surveyed.



Duty of care for known scams

Within the dynamic landscape of financial security, banks are increasingly confronted with scenarios where safeguarding customer assets intersects with customer autonomy. We asked the banks what actions they take when a customer insists on proceeding with a transaction that's been flagged as a potential scam. The responses showed a variety of strategies designed to mitigate the risks with balancing customer relations.

- **Blocking transactions:** The results show 51% of banks elect to block transactions that could be unmistakably linked to a scam, such as those with blacklisted recipients.
- **Informed consent:** Some banks obtain explicit consent from customers they detected as being at impending risk of a scam. This involves a verbal or written confirmation, acquired in-person at a branch or by signing a release form. In both instances, the customer acknowledges the risks and absolves the bank from the financial consequences of the transaction. This ensures customers are fully aware of the dangers and that the bank has exercised due diligence in its advisory role.
- **Adding friction:** Some banks add further friction that forces customers to pause, providing time to change their minds about an APP scam. This might include detailed questions to help the customer reassess the transfer, sending customers to a branch or advising customers to seek the opinions of trusted family members.
- **Risk profiles and proportionate responses:** Banks often tailor their response to the perceived level of risk associated with a scam or fraud. For instance, small and perceived lower-risk transactions might be processed after the customer is educated. But transactions with a higher risk or value are more likely to be refused.
- **Escalation and law enforcement:** In cases where the scam is clear-cut and the customer remains undeterred, some jurisdictions will escalate the matter to law enforcement. In the UK, the banks and police have joined forces in a rapid response scheme called the Banking Protocol. Under the scheme, branch staff are trained to detect the warning signs that a customer is being scammed and will call emergency services. Police will visit the branch to investigate the suspected fraud and arrest any suspects still on the scene.
- **Prioritising customer choice:** Banks that will process a flagged transaction at the customer's wishes based this policy on their own reputational and legal risks, and the customer's ultimate authority to act.

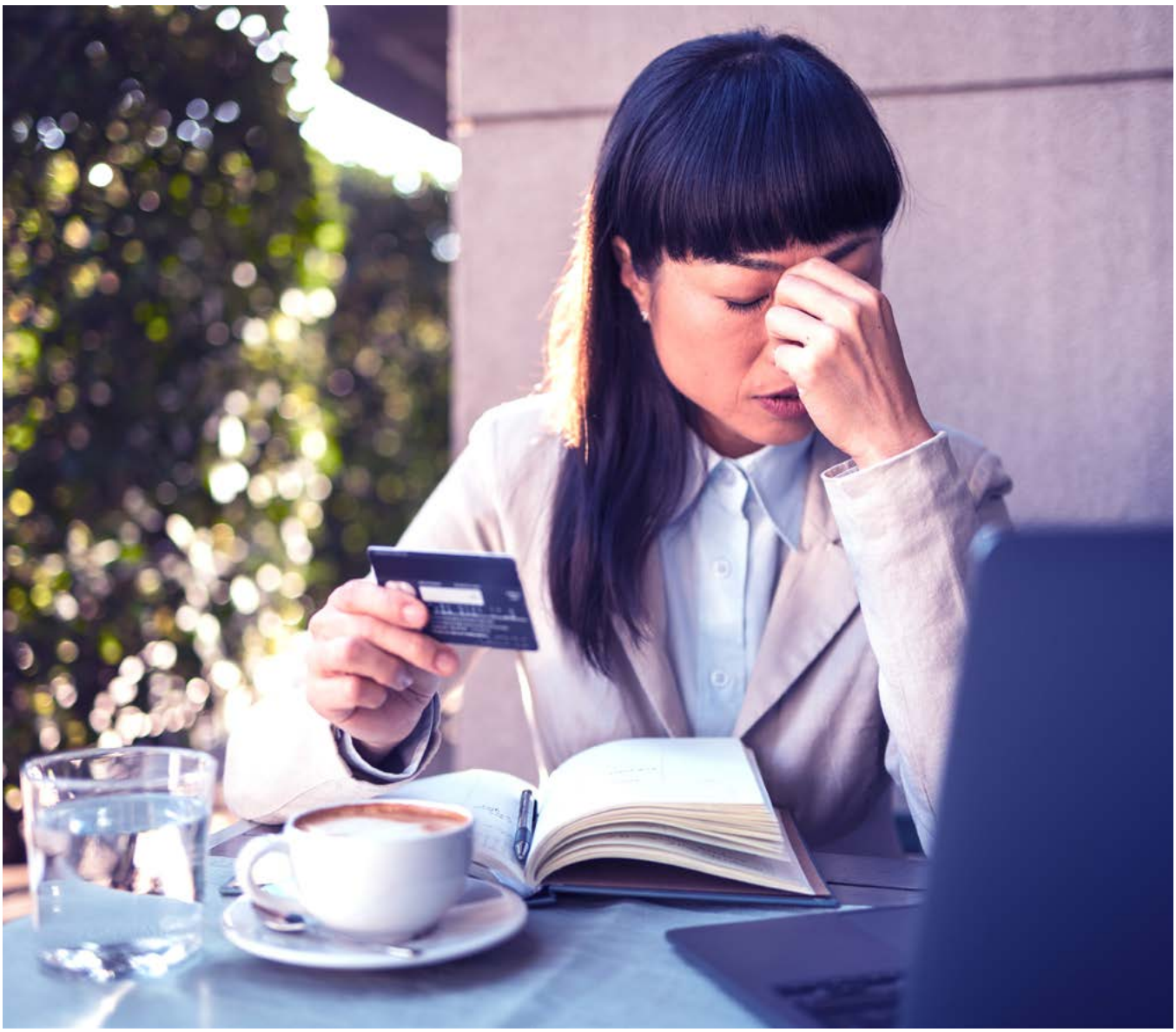
Duty of care for repeat victims

A significant consideration for banks is whether to continue servicing customers that are repeat scam victims or to off-board them because of the heightened risk and operational costs.

Most banks surveyed preferred to take protective measures over outright off-boarding customers. Applying markers or enhanced scrutiny to the accounts of repeat victims allowed banks to proactively monitor for fraudulent activity without severing the relationship. This also often involved adding transactional friction to safeguard both the customer and the bank from further scams.

Rather than closing accounts, some banks apply specific restrictions, such as limiting access to online banking or international transactions. This approach has helped to reduce exposure to fraud while supporting customers by maintaining essential banking services. The issue of financial inclusion is a significant influence on this decision-making process.

Although 45% of banks say they'd off-board consumers as a last resort, it's not common practice. It's usually an executive-level decision made on a case-by-case basis. This measure is taken when evidence suggests that the risk – including potential complicity in fraud (known as first-party fraud) – doesn't justify continuing the account. Most banks are cautious about denying banking services and only consider off-boarding if the customer has deliberately engaged in fraudulent activities.



6. Intelligence

Most of the banks share some form of APP scam intelligence as part of a consortium data approach to combating scams and fraud.

The organisations and approaches included:

- **Partnerships with law enforcement:** Some countries have dedicated financial crime units, such as Singapore Police Force's Anti-Scam Command and the UK's National Economic Crime Centre within the National Crime Agency.
- **Industry associations:** These associations include UK Finance, Nordic financial CERT and Canadian Bankers Association, Nederlandse Vereniging van Banken (Dutch Banking Association), The American Bankers Association and the Australian Bankers Association.
- **Private partnerships:** Globally, the finance sector has several partners that provide consortium data sharing.
- **Not-for-profit organisations:** Examples include UK's Cifas, the Australian Financial Crimes Exchange (AFCX) and the South African Banking Risk Information Centre (SABRIC).

The amount of information shared was varied and some banks reported limitations due to privacy barriers, data privacy regulations like GDPR, or national central bank policies. This is considered a priority area for future action due to the cross-border nature of scams.

7. Brand protection

In today's digital landscape, protecting a bank's brand is essential. Strong brand protection ensures customer confidence, reinforces security measures, and upholds the bank's reputation.

Dark web monitoring

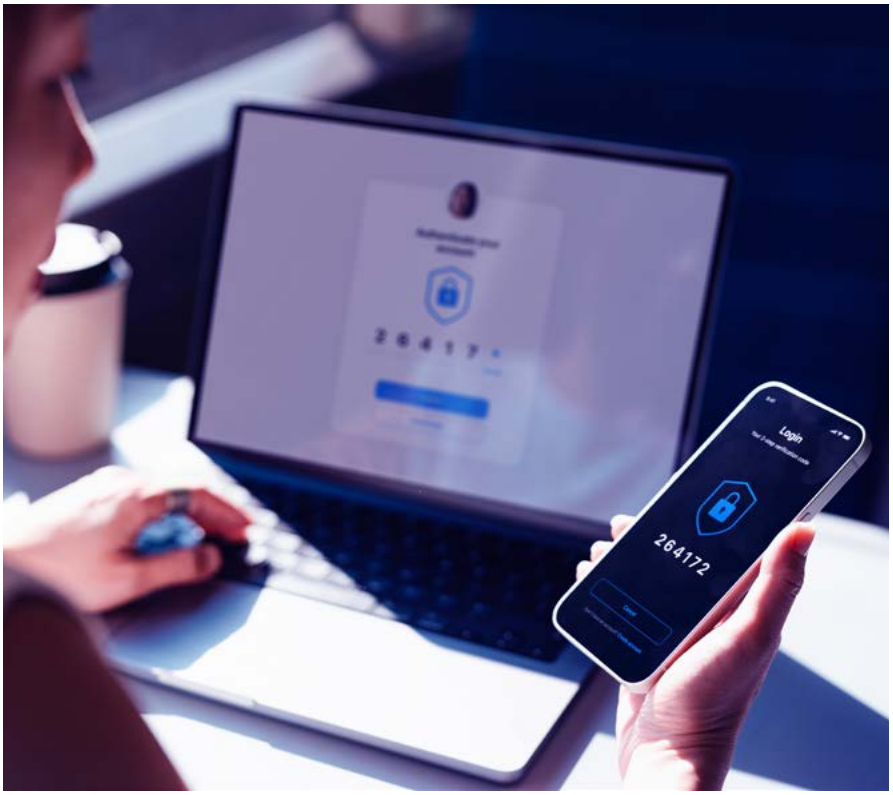
A significant 83% of the banks we surveyed monitor the dark web for intelligence on scams. The bank's cyber security teams (or engaged vendor) monitor for:

- **Scam trends** including instances where the bank itself is named or identified.
- **Compromised customer information** including card details.
- **Data leakage** of unauthorised sensitive or personal information.
- **Reputational intelligence** looking for general chat about the bank.

Other activities

Other initiatives the banks have implemented to protect their brands from scam or fraud-related compromise include:

- **Impersonation:** Banks monitor the internet for copyright infringements, copied website code, clones, fake mobile applications and social media mimicking the bank or its staff. Internet domains related to the bank's name can be monitored for registrations that may indicate the existence of fake websites.
- **Alpha tag protection:** Alpha tags enable banks to send branded one-way text messages to customers. Some banks are working with telecommunications providers and global trade associations to protect their alpha tags from spoofing (where a scam text appears to have come from a legitimate sender ID).
- **Takedown services:** These services help remove harmful content from the internet. They're typically a third-party provider that helps banks, other businesses and individuals remove content that violates their brand, copyright or privacy. Their activities can include removing fake marketing websites or social media profiles.
- **White hat hackers:** These are also known as ethical hackers and are cyber security professionals. They apply their expertise to detect and rectify security flaws in systems, networks and applications. White hat hackers operate with the consent of system owners, enhancing security measures and safeguarding against potential risks.
- **Do not originate lists:** These lists contain inbound numbers that banks use and may be likely to be spoofed. Some banks place their numbers on 'do not originate lists' to prevent scammers from impersonating their numbers.



8. Technology

As scams continue to evolve, so does the technology used to prevent, detect and respond to APP scams.

Orchestration layers

Orchestration layers integrate multiple data sources into a single system, enhancing accessibility to client information enabling faster and more accurate decision-making, as well as easier interrogation in the case of cyber incidents.

'A review across client activities (360-degree view) and not just a single transaction is the strongest control.'

Of our respondents, 59% of banks said they have an orchestration layer, with several banks currently building or implementing one.

Data sources that were integrated included:

- transaction data
- KYC information
- risk ratings
- device intelligence
- behavioural analytics
- fraud alerts.

'The customer's behaviour trends at different levels, transaction habits and profile characteristics can be evaluated together.'

'We know that 99% of all frauds aren't opportunistic. They are connected to something else and are well organised; therefore, the bank cannot look at things in isolation. They need to make sure that they understand the connections between transactional and non-transactional information.'

Next-generation protection technology

The survey participants provided a variety of insights on what they considered will become the next-generation anti-APP scam technologies:

- **Behavioural analytics:** These are mostly used to detect unauthorised scams. There has been success in using behavioural biometrics to detect stress in customer voices, which may indicate they're potential scam victims.
- **Deepfake detection:** Banks are using a range of tools to identify and prevent identity deepfake-based fraud.
- **Dynamic and self-learning rule setting:** Systems that can adapt and update fraud detection rules based on continuous monitoring or transaction data, dynamic rules evolve in real time and can quickly respond to new scam typologies.
- **Dynamic warnings:** Banks would like to see more assertive and specific language used during the payment journey so customers understand why a particular transaction is a risk of scam or fraud. These may include automated and Gen AI -driven interactions with the customer before the transaction occurs.

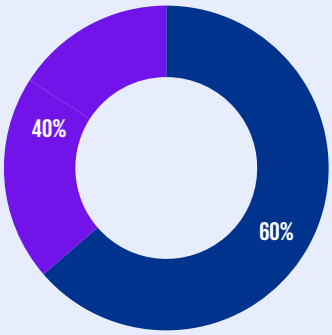
9. Customer complaints

Trends observed in customer complaints about fraud and scams.

- **Reimbursement:** These occur when customers don't receive refunds or are dissatisfied with the outcome of their reimbursement claims.
- **Friction:** Customers express frustration with the number of restrictions when trying to resolve a complaint or complete a transaction. These restrictions include delays, blocks and perceived excessive security measures.
- **Protection:** Some customers felt the banks should do more to prevent APP scams from occurring. The protection measures they seek include better detection, more effective education efforts and blocking potential scam transactions.
- **Resolution:** Additional concerns include slow turnaround times from initial complaint to resolution, availability of funds and poor communication from the bank with updates on scam cases.

One bank has seen an increase in complaints from criminals. 'The criminal will try to go to branch to force the branch to lift the hold on the account.'

Have you seen an increase in scams related customer complaints?

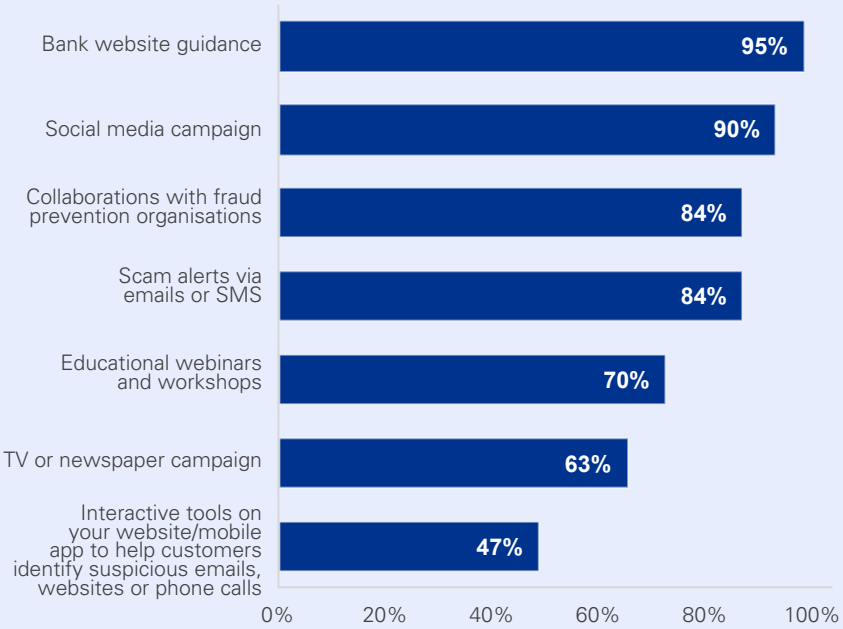


10. Customer education and awareness

By providing education about the signs and tactics of APP scams, banks hope that customers become more vigilant and better equipped to protect themselves and question suspicious requests.

To better understand the role of customer education and awareness in scam prevention, we asked banks to indicate whether they had implemented any of seven specific initiatives.

Which of the following initiatives have you implemented?



Among all banks, it was felt the communication strategy needed to be a process of continual engagement across multiple platforms, rather than a single effort. A few banks said campaigns are only effective for a short time.

Some of the innovative approaches we heard about from the banks based on both their own approaches and what they'd observed in the market were:

- collaborations with central banks and universities
- informing customers of fraud trends while they are on hold to bank contact centres
- seasonal initiatives targeting holidays such as Christmas or Eid
- targeted campaigns highlighting risks with online marketplaces
- making pop-ups specific to transactions to counteract pop-up fatigue
- making customers do an e-learning module on cryptocurrencies before they were allowed a digital wallet.

'In 2024 alone, 32 awareness campaigns were conducted.'

Scam warnings and education

Despite challenges with quantifying their benefit, 51% of banks confirmed they try to monitor the efficacy of their scam warnings and educational activities.

Methods to measure the effectiveness of these activities include:

- **Measuring penetration:** viewers, listeners and click rates.
- **Impact of warnings on payment journeys:** payments abandoned after targeted warnings were shown.
- **Anecdotal evidence:** success stories from customers who successfully avoided fraud.
- **Analysing scam trends** after educational campaigns.
- **Client surveys** and feedback.

11. Challenges and opportunities

We asked banks to identify future challenges and opportunities in APP scam risk management. Similar themes emerged for both.

THEME	CHALLENGES	OPPORTUNITIES
Regulations	The pace of regulatory change is considered a significant challenge, as banks must adapt to rapidly changing environments across multiple jurisdictions. Non-banking companies within the scam ecosystem were perceived to be less accountable to regulatory requirements than banks in many jurisdictions.	Strengthening regulations and tailoring successful regulatory models from other countries to fit local contexts could ensure their effectiveness and relevance. Enhanced regulation across all stakeholders in the scam ecosystem and fostering collaboration will help all industries identify and combat APP scams.
Data sharing	It was felt that data privacy regulations may sometimes hinder the ability to share critical information. This is especially difficult with cross-border transactions. The globalisation of transactions and international crime syndicates further complicate cooperation between banks and law enforcement in different countries.	There's opportunity for a comprehensive strategy to effectively combat fraud and money mule networks involving transnational partnerships and consortium data modelling. This approach could encompass cross-sector data-sharing protocols and collaboration among banks, law enforcement, telecommunications companies, cryptocurrency exchanges and other key ecosystem players.
Technological advancements and AI	The rise of Gen AI is expected to further complicate scam detection as it enables fraudsters to craft more sophisticated and convincing schemes, including bypassing basic customer identification measures.	Gen AI can help in scam risk management. For example, it could create tailored interactions to alert customers to specific risks.
Customer awareness and education	There was an acknowledgement of 'message fatigue' amongst customers. Banks need to think of new ways to deliver the messages.	There's an opportunity for government-funded campaigns to increase public awareness and empower customers to protect themselves with critical thinking and stronger authentication measures.
Investment in technology and resources	There needs to be continuous investment in new tools and training so banks can keep up with evolving scam techniques. The competition for skilled human resources and the migration of talent in some countries pose additional challenges.	Banks could consolidate anti-fraud operations and leverage machine learning to optimise fraud detection processes.
Single view of the customer	Some banks found it hard to have a broad view of the customer across all channels and products, preventing them from proactively identifying scam behaviour.	Banks are moving to consolidate data collection into an orchestration layer with Gen AI enabled teams to handle multiple functions.

12. Contacts and contributors

We'd like to acknowledge the contribution of the following individuals across KPMG member firms who assisted in the development of this publication.

Trygve Kringlebotn Aandstad
Director, Forensic
KPMG in Norway
E: trygve.aandstad@kpmg.no

Marilyn Abate
Partner, RC – Financial Crimes
KPMG in Canada
E: marilynabate@kpmg.ca

Steve Ackroyd
Director, Forensic I&C
KPMG in the UK
E: steve.ackroyd@kpmg.co.uk

Ignatius Adjei
Partner, FS Forensic
KPMG in the UK
E: ignatius.adjei@kpmg.co.uk

Anja Apfel
Assistant Manager -
FS Regulatory & Compliance
KPMG in Germany
E: aapfel@kpmg.com

Maria Barcenilla
Director, Forensic Technology
KPMG in Spain
E: mbarcenilla@kpmg.es

Cedric Biedermann
Director, CO Forensic CH
KPMG in Switzerland
E: cbiedermann@kpmg.com

Luca Boselli
Partner, Forensic
KPMG in Italy
E: lboselli@kpmg.it

Christina Chliaoutaki
Manager, Data Analytics
KPMG in Greece
E: cchliaoutaki@kpmg.gr

Pedro Costa
Partner, Advisory
KPMG in Portugal
E: pdcosta@kpmg.com

Mikael Flod
Senior Manager, Financial Services
KPMG in Sweden
E: mikael.flod@kpmg.se

Patricia Gabriel
Associate Director, RC GRC
KPMG in South Africa
E: patricia.gabriel@kpmg.co.za

Joakim Hansson
Manager, Financial Services
KPMG in Sweden
E: joakim.hansson@kpmg.se

Christopher Jackson
Director, Forensic
KPMG in Singapore
E: christopherjackson@kpmg.com.sg

Marc Kilcher
Partner, FS GE
KPMG in Switzerland
E: mkilcher@kpmg.com

Eric Lachapelle
Partner, RC – Financial Crimes
KPMG in Canada
E: ericlachapelle@kpmg.ca

Alex Lerner
Senior Associate, Financial Services
KPMG in USA
E: alexlerner@kpmg.com

Alwyn Loh
Director, Forensic
KPMG in Singapore
E: alwynloh@kpmg.com.sg

Joao Madeira
Partner, Advisory
KPMG in Portugal
E: jmadeira@kpmg.com

Michelle van der Merwe
Senior Manager, Forensic
KPMG in South Africa
E: michelle.vandermerwe@kpmg.co.za

Javier Migoya
Director, Forensic Technology
KPMG in Spain
E: jmigoya@kpmg.es

Oytun Onder
Partner, Forensic
KPMG in Turkey
E: oonder@kpmg.com

Patrick Ozer
Partner, Forensic
KPMG in the Netherlands
E: ozer.patrick@kpmg.nl

Catherine Pihl
Manager, Forensic
KPMG in Norway
E: cathrine.pihl@kpmg.no

Timo Purkott
Partner, Forensic
KPMG in Germany
E: tpurkott@kpmg.com

Jori van Schijndel
Senior Manager, Forensic
KPMG in the Netherlands
E: vanSchijndel.Jori@kpmg.nl

Paul Stanwix
Associate Director, Forensic
KPMG in Australia
E: pstanwix@kpmg.com.au

Harriet Tennent
Director, Forensic
KPMG in Australia
E: htennent1@kpmg.com.au

Cenk Tuce
Director, Forensic
KPMG in Turkey
E: ctuce@kpmg.com

Dustin J Tupper
Managing Director, Advisory
KPMG in USA
E: dtupper@kpmg.com

Vasiliki Varzaka
Director, Deal Advisory
KPMG in Greece
E: vvarzaka@kpmg.gr

Amelia Ventura
Associate Partner, Forensic
KPMG in Italy
E: aVentura@KPMG.IT

Rohan Vinu
Manager, Forensic
KPMG in Australia
E: rvinu@kpmg.com.au

KPMG.com.au

February 2025. 1533063575CON