ACI Worldwide®

GlobalData.

2024 Scamscope

The Battle for Trust

APP scam trends in the U.S., the U.K., Australia, India, Brazil, and the UAE

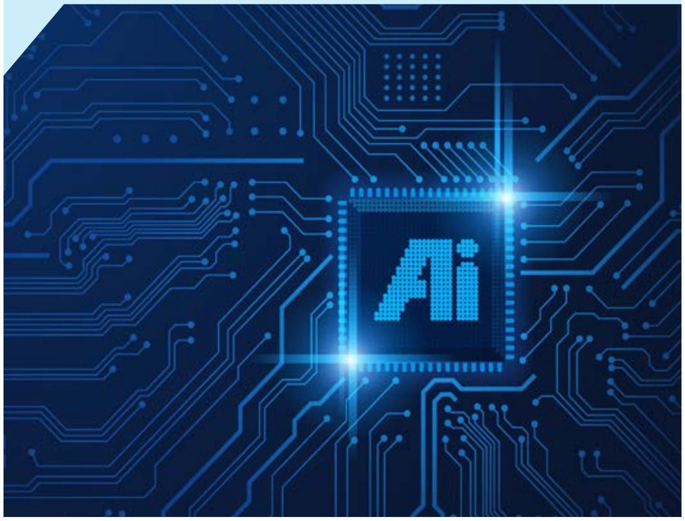
A report by ACI Worldwide and GlobalData

Table of contents

Executive summary

The battle for trust is on. Precision and intelligence will win the war on scams.

> “Beating scammers requires shared responsibility and systems that eliminate the opportunity for criminals while enriching legitimate consumer experience. By using collective intelligence to fight back, governments, banks, and businesses can not only reduce financial losses but, more importantly, restore public trust.”
>
> **Cleber Martins**
> Head of Payments Intelligence & Risk Solutions
> ACI Worldwide



The growth of APP fraud is a call to action for banks

APP fraud is now ubiquitous across every market, preying on emotions and eroding the trust between people and institutions. Beyond financial loss, scams can destroy reputations, relationships, security, and ambitions.

In all the countries featured in this year’s report, scam values are on the rise. Many romance, confidence, and investment scams carry social stigma and often go unreported, suggesting that the true figures are likely to be much higher.

Scammers are getting bolder and faster

Scammers are leveraging advanced technology to launch more sophisticated attacks at scale. They are using AI to boost inherited trust to unprecedented levels—automating hits; improving scam content, scope, and reach; and driving more effective social engineering techniques. And they are also reaping the rewards more easily, using synthetic identities to set up receiving accounts that bypass traditional controls.

Added to this is the rise of real-time payments, which has reduced the window of opportunity to spot and stop scams. Our data reveals that APP fraud through real-time payments is predicted to increase from 63% of all APP fraud losses in 2023-2024 to 80% by 2028.

Banks must use intelligence to combat fraud

FIs have heavily invested in multifactor authentication. This has effectively cut many types of financial fraud. But these measures fall short in combating APP scams, where transactions are authorized by the legit account holder.

In response, governments are stepping in. They recognize APP scams as a pressing social issue. Regulators are starting to enforce stricter rules to hold banks accountable for scam-related losses and pushing FIs to adopt more sophisticated monitoring systems that track both outgoing and incoming transactions.

To meet these challenges, spot trends, and shut down scammers, banks must “fight fire with fire” by leveraging AI to help analyze transactional data, flag suspicious behaviors, and facilitate real-time collaboration with other banks.

Debunking mule accounts remains a priority

In last year’s Scamscope report, we highlighted the urgency of shutting down mule accounts. This remains a critical area of focus in 2024.

Scammers are opening accounts using synthetic identities fueled by dark web data—or buying or extorting them from legitimate account holders. Traditional fraud prevention methods, such as transaction limits or account blacklists, are not effective.

Banks can raise their game by ensuring seamless integration between their anti-money laundering (AML) and anti-fraud functions, both in real time. They can also use AI to analyze current transaction signals and behaviors to make decisions based on immediate risks rather than outdated data.

As banks face increased accountability for mule accounts that enable scammers to profit, regulations like the U.K.'s mandate for banks to reimburse victims of APP scams—with 50% liability on the receiving bank—will set a precedent for others to follow.

The power of collective intelligence

Across regions, there is a growing emphasis on collective intelligence and cross-industry collaboration.

By enriching transaction data with insights from partners like telecoms and social media platforms—and exchanging intelligence in real-time with peers, central infrastructures, and subject matter experts like ACI—banks can create a more comprehensive fraud detection framework. This intelligence network facilitates quicker identification of fraudsters and alleviates the burden on individual institutions, fostering a safer environment for customers while reducing associated costs.

Fraud prevention signals can also provide valuable insights for other departments within banks, such as AML, marketing, and customer experience. By applying predictive models across various industries, fraud prevention competencies in precise decision-making can transform into a strategic asset.

Creating actionable insights

Open finance initiatives are revolutionizing how financial data are shared across institutions. However, raw data alone are insufficient; domain knowledge and a consistent methodology for interpreting data are essential to extracting actionable insights. A standardized approach to data interpretation and predictive correlation will enable the effective sharing of intelligence signals across industries and facilitate their application to various use cases, preserving privacy, and enforcing legitimate interest.

There is a striking parallel between the internet's democratization of knowledge and AI's ability to democratize intelligence. It can provide business users with predictability and all the capabilities of a data science expert. By connecting AI systems across sectors, predictive intelligence signals can be rapidly disseminated, empowering businesses to enhance fraud detection, improve customer experiences, and deliver value across financial services, retail, insurance, and more.

The future: building a coordinated defense

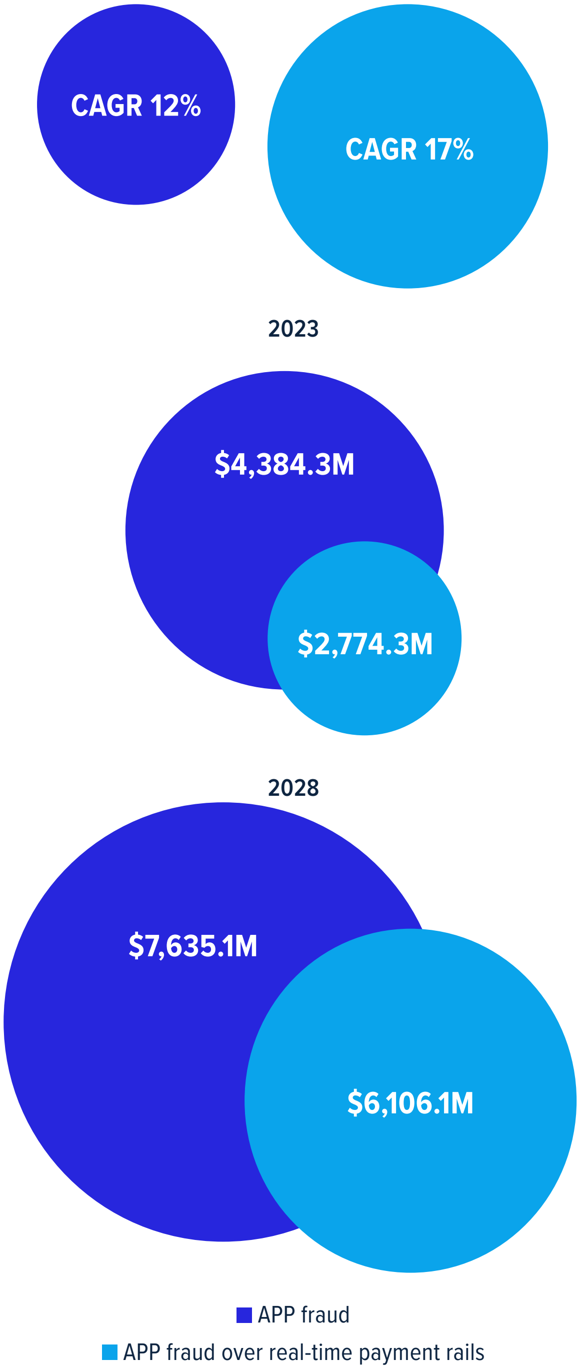
Scammers' war on trust will continue. Looking ahead, there is a clear need for increased accountability, especially concerning the receiving end of transactions. In the next two to three years, we can anticipate a widespread adoption of predictive intelligence exchanges across industries, leading to enhanced fraud detection and improved user experiences, enforced by regulations or, preferably, led by responsible and innovative financial communities taking proactive action.

To truly combat APP fraud, the goal must be to establish a consistent methodology for sharing intelligence among institutions, enabling a coordinated and effective defense and rebuilding public trust.

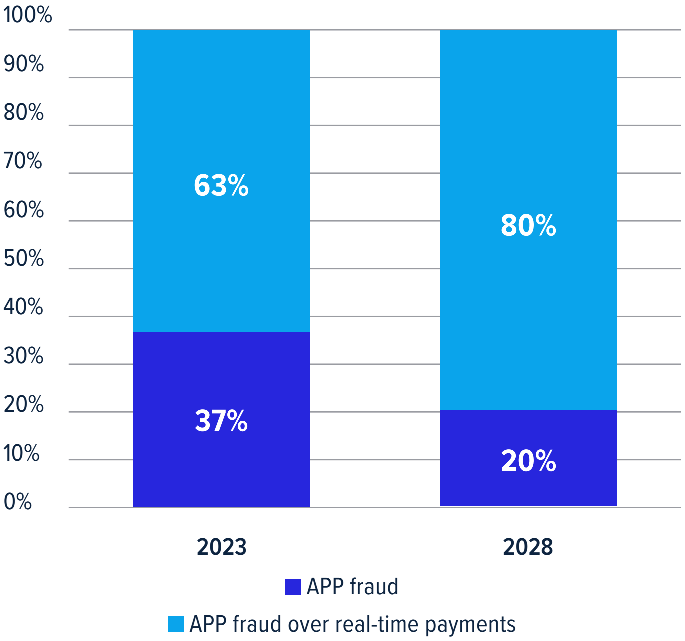
Cleber Martins
Head of Payments Intelligence
& Risk Solutions
ACI Worldwide

A global snapshot

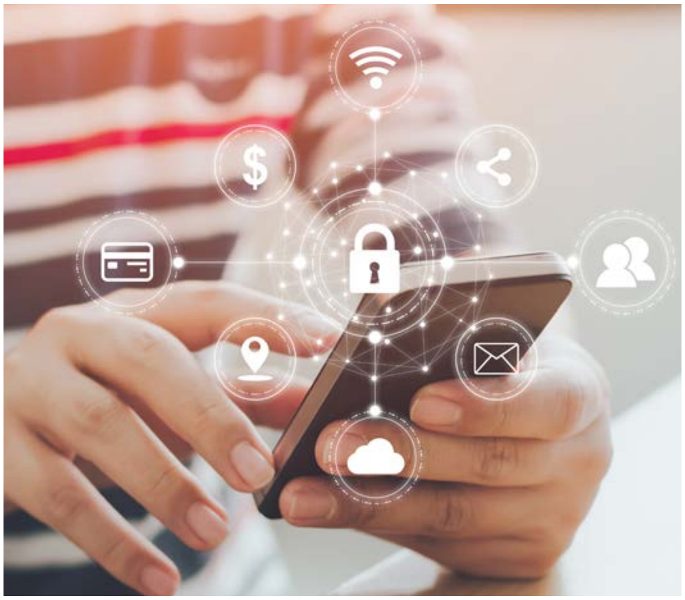
APP scams over real-time payment rails are increasing faster than overall APP scams from 2023-2028



APP fraud losses through real-time payments (as a percentage of overall APP fraud losses) are predicted to increase from 63% in 2023 to 80% in 2028, an increase of more than $3.3 billion in value.



Global neutral outlook, APP fraud versus APP fraud over real-time payments in USD
(*local currency units can be found within country sections*)

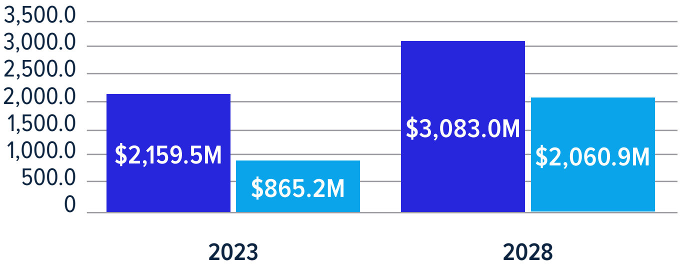


ACI Worldwide®

Global snapshot

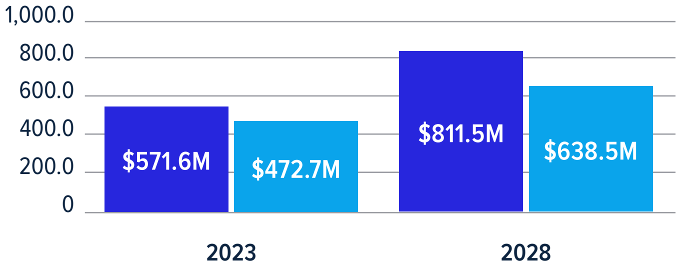
Accelerated APP scams over real-time payment rails by country

U.S.



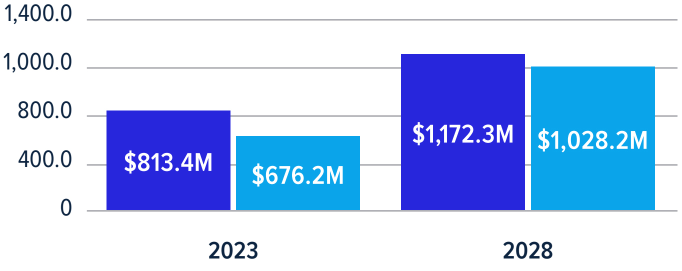
~19% growth in value of APP scams over real-time payments

U.K.



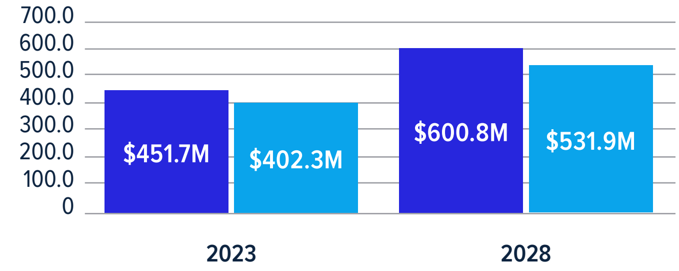
~6% growth in value of APP scams over real-time payments

Australia



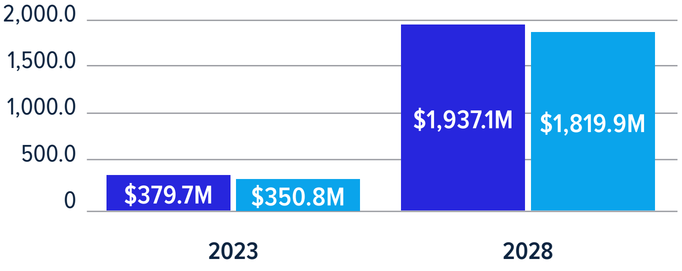
~9% growth in value of APP scams over real-time payments

India



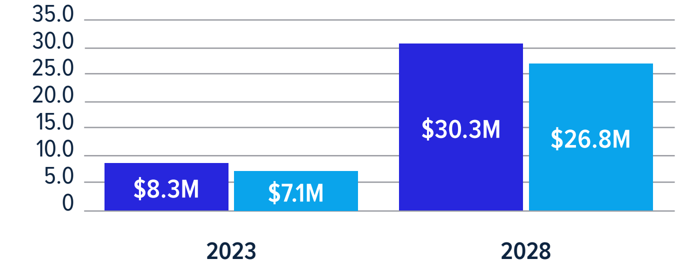
~6% growth in value of APP scams over real-time payments

Brazil



~39% growth in value of APP scams over real-time payments

UAE



~30% growth in value of APP scams over real-time payments

■ APP fraud value of transactions (USD millions)

■ Real-time payments APP fraud value of transactions (USD millions)

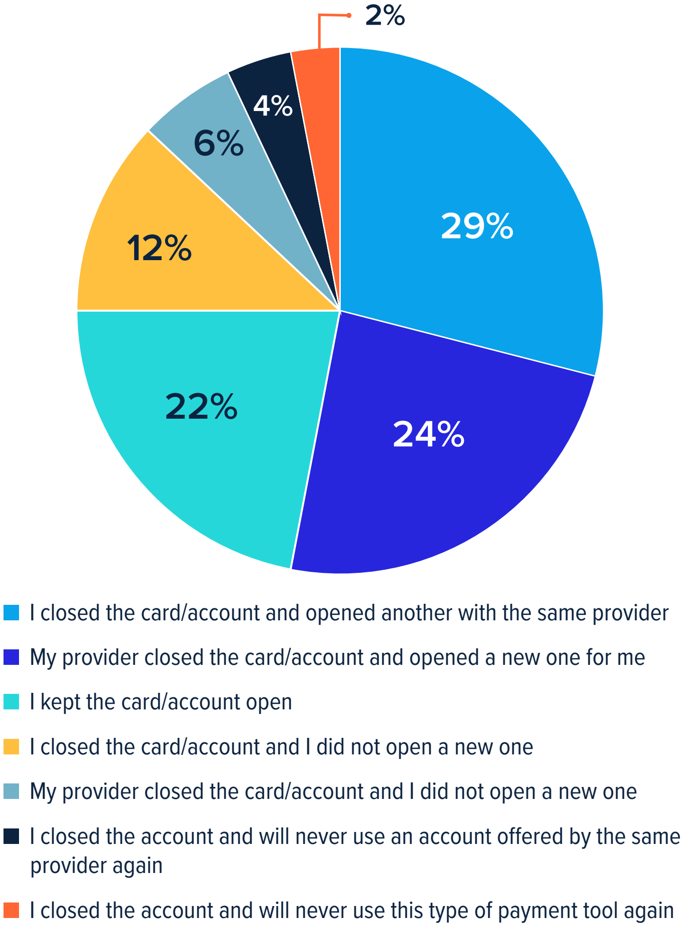
Global snapshot

The requirement for vigilance from the sending end to the receiving end

18% Purchase scams	**18%** Investment scams	**18%** Advance payment scams	**15%** Impersonation scams
11% Invoice scams	**9%** Authority scams	**7%** Romance scams	**4%** Other

Globally, financial institutions need to educate their consumers to be vigilant when coming across advance payments, impersonation, and purchase scams. One in two victims have fallen as prey to these scams, directly impacting the trust on a financial institution.

Trust snapshot: 1 in 4 victims chose to walk away from their current financial institution



Country insight: U.S.

ID verification is key to breaking the U.S.' scam cycle

Across the U.S., scammers are taking advantage of American prosperity, with our report showing that impersonation, advance payment, and investment scams are reaping them the highest rewards. Romance scams are also prominent and have overtaken authority and purchase scams in terms of value.

A significant portion of scam money leaves the country, while the other portion goes to domestic criminal organizations, including small "mom and pop" operations. It's evident that continuous data breaches in the U.S. have made it easy for scammers to obtain and resell personal information. Generative AI is also making it easier for overseas organizations to target individuals in the U.S. by improving language, etc.

The popularity of faster payment channels is driving urgency

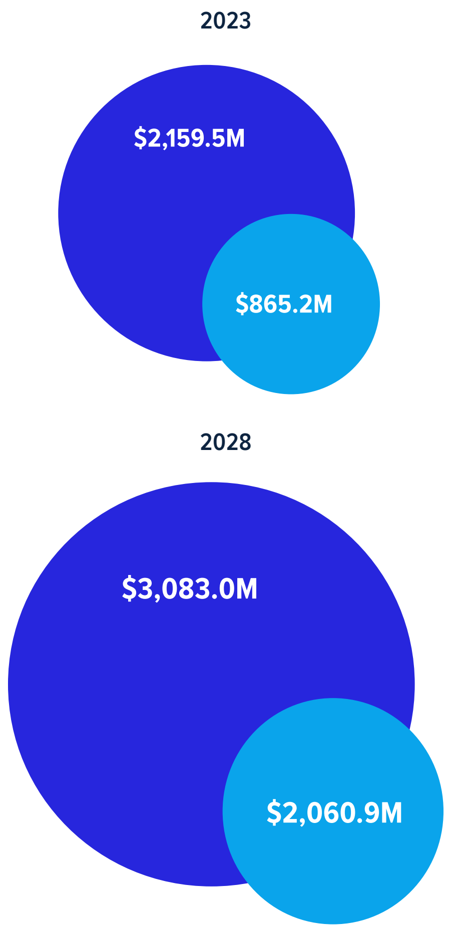
The U.S. Faster Payments Council estimates that by 2028, between 70% and 80% of all U.S. FIs will be enabled to receive real-time payments, and between 30% and 40% of FIs will be enabled to send instant credits. High-volume use cases include invoicing, government payments, taxes, wallet funding, online banking, and gaming.

This makes them prime targets for scammers eager to take advantage of spontaneous purchase behaviors and rapid processing speeds which make it hard to recall a transaction and get the money back.

In the U.S., the onus is mostly on the financial service providers to have strong fraud risk controls. While older systems and digital wallet networks like Zelle, Venmo, and CashApp have established controls, these are clearly not enough to combat real-time scammers. And while TCH and the FedNow® Service provide strong fraud management capabilities, these are still evolving and are dependent on banks adopting best practices.

Obviously, there is still a lot of work to be done, but the relatively recent launch of the FedNow Service gives banks a chance to enhance customer education about the risk of real-time payments. Banks can also use the FedNow Service investment to support more sophisticated fraud detection systems—including real-time transaction monitoring, AI, and machine learning tools—to identify unusual patterns indicative of fraud.

Growth of APP scams vs. APP scams over real-time payments



CAGR 7% APP

CAGR 19% APP over real-time payments

■ Losses to APP fraud

■ Losses to APP fraud over real-time payments

Country insight: U.S.

There are inherent weaknesses in the system

Real-time payments have highlighted many of the inherent weaknesses in older faster payment systems. Scammers often use the same approaches and tactics across multiple organizations and payment rails to convince victims to send authorized payments.

According to the Federal Reserve's Scams Information Sharing Industry Work Group, the U.S. payments industry lacks real-time access to current, industrywide information necessary to develop effective strategies to detect and prevent scams.

For some banks, there is a lack of motivation to tackle scam detection and prevention due to no clear liability, perceived complexity, and other urgent modernization priorities. Meanwhile, smaller institutions often lack the mindset, desire, and capability to actively invest in robust fraud detection measures.

Importance of digital identity in breaking mule accounts

Identifying U.S. mule accounts remains a major issue. There is an overreliance on credit bureaus for identity verification, and business models allow fraudsters to create new credit files with minimal checks.

Scammers are also using synthetic identities to open accounts. These may use real data points but often involve changing details like dates of birth and addresses, which current systems fail to detect. This highlights the need for a robust digital identity system to combat fraud.

U.S. banks are starting to address synthetic identity fraud to help break the cycle of money laundering through mule accounts. But addressing the issue with identity verification models requires industrywide collaboration or government mandates. If the U.K. takes the lead in implementing a digital ID system, the U.S. could follow.

Scam renumeration and liability remains fragmented

Currently, there is no federal mandate specifically requiring reimbursement for victims of scams. However, various federal and state agencies do provide resources and support for victims. Under certain circumstances, FIs may be held liable for losses resulting from scams, particularly if they failed to comply with regulations designed to protect consumers.

Regardless of liability, banks have an interest in fixing the problem due to the reputational risk and potential for customers to leave en masse. Education of consumers and the industry is seen as key to tackling scam-related fraud.

ACI is involved in the U.S. Federal Reserve's scam definition and classification working group. This aims to create a standardized model for classifying scams to improve scam detection, reporting, and mitigation, ensuring consistent application across the industry.

Nearly 2 out of 5 victims were coerced into making an authorized payment via impersonation or asked to make an advance payment

18% Impersonation scams

18% Advance payment scams

14% Investment scams

14% Invoice scams

12% Romance scams

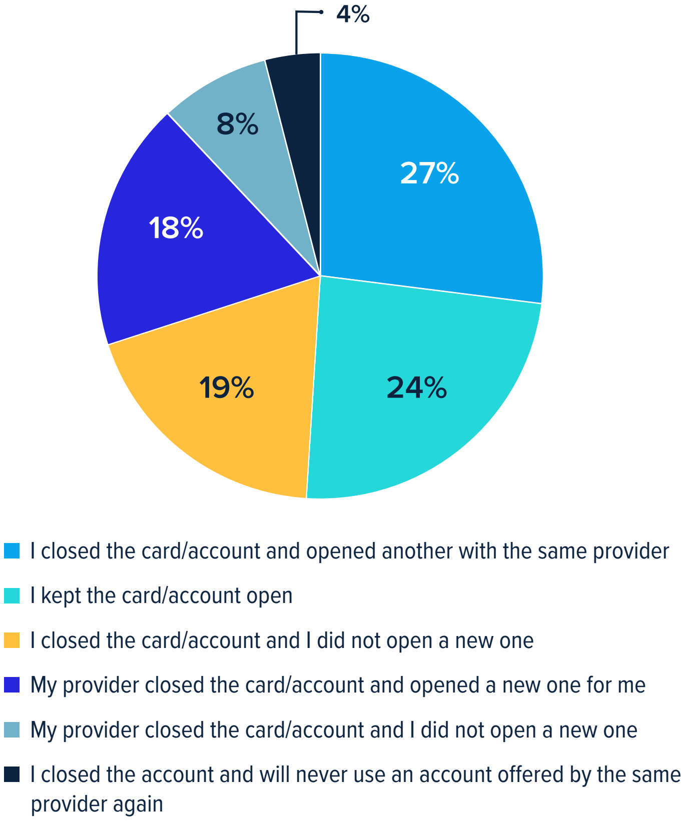
11% Purchase scams

11% Authority scams

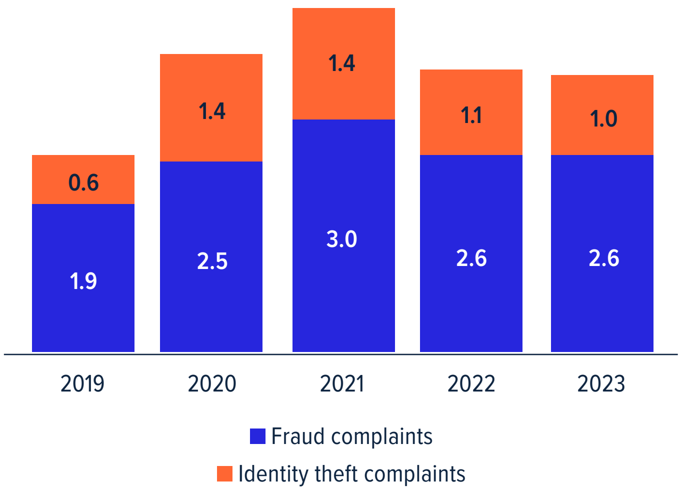
2% Other

Country insight: U.S.

More than 30% of victims chose to not continue with their existing financial institution, negatively impacting consumer trust and confidence

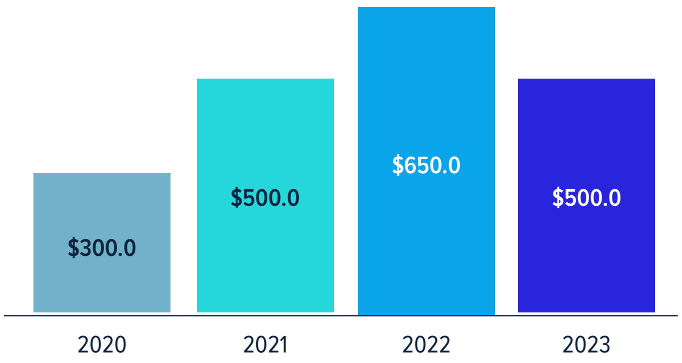


Number of reported complaints (million)[1]



The number of fraudulent activities increased in the U.S. during 2021. The growth between 2019 and 2023 has been notable, with fraud complaints rising by 135% and identity thefts increasing even more significantly by 160%.

Median loss ($)[1]



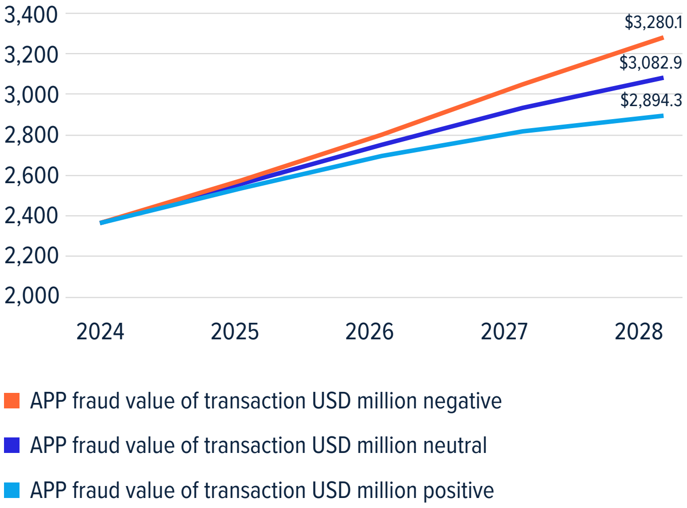
Considering the total loss and the number of fraud reports, the median loss in the U.S. grew significantly in 2021 compared to 2020, with an increase of 67%. It rose further in 2022, with a 30% increase compared to 2021. In 2023, the median loss was $500.0, similar to the value in 2021.

[1] *Source: Federal Trade Commission, Consumer Sentinel Network*

Country insight: U.S.

Forecasting the evolution of scams in the U.S.

Regulatory inertia holds U.S. AI adoption back



Conclusion: The U.S. is at a critical crossroads. With scammers leveraging sophisticated techniques and generative AI, FIs must prioritize innovation in fraud detection and prevention. As scams evolve, regulators may be prompted to reevaluate existing frameworks related to bank liability and consumer protection. Discussions about ID verification, industry sharing, and more stringent AI-based fraud prevention measures are likely to dominate the legislative agenda in the year to come.

In 2023, the U.S. lost more than $2 billion to consumer APP fraud alone. The U.S. is also a hotspot for card fraud (losses of more than $13 billion in 2023). As the U.S. Federal Reserve's FedNow Service brings real-time payments to the country, scams will become a more significant threat to consumers and FIs. The stakes are high: more than 30% of consumers who fall victim to scams report ending their relationship with the bank involved, compounding APP losses with revenue and reputational damage.

Looking ahead, consumer scams in the U.S. are projected to exceed $3 billion by 2028. While AI-based anti-fraud measures could help mitigate these losses, conversations with U.S. compliance professionals suggest that regulatory pressure for banks to adopt AI is unlikely. Compliance costs are already high, and even with enhancements, our best-case scenario indicates only a modest saving of $388 million in APP fraud losses by 2028. Clearly, more fundamental changes are needed to drive significant transformation in this area.

Consumer survey base: 84 scam victims

Country insight: U.K.

Leading the way in consumer protection with new reimbursement models

According to Ofcom, 87% of U.K. adult internet users have encountered content online which they believed to be a scam or fraud – and nearly half (46%) have engaged with them.

The good news is that efforts applied by U.K. banks have had a positive impact on fraud. Although there has been a notable increase in APP fraud cases, there has been a slight decrease in overall financial losses, indicating more effective fraud prevention measures and lower losses per case.

But APP fraud remains a major issue. Scammers are becoming increasingly proficient in deceiving consumers into thinking websites, apps, and payment requests are legitimate. This is leading to high levels of growth in product and purchase scams. Trust scams are also experiencing a significant uplift as scammers use AI to fine-tune attacks and make it even harder for victims to spot fake content and sources.

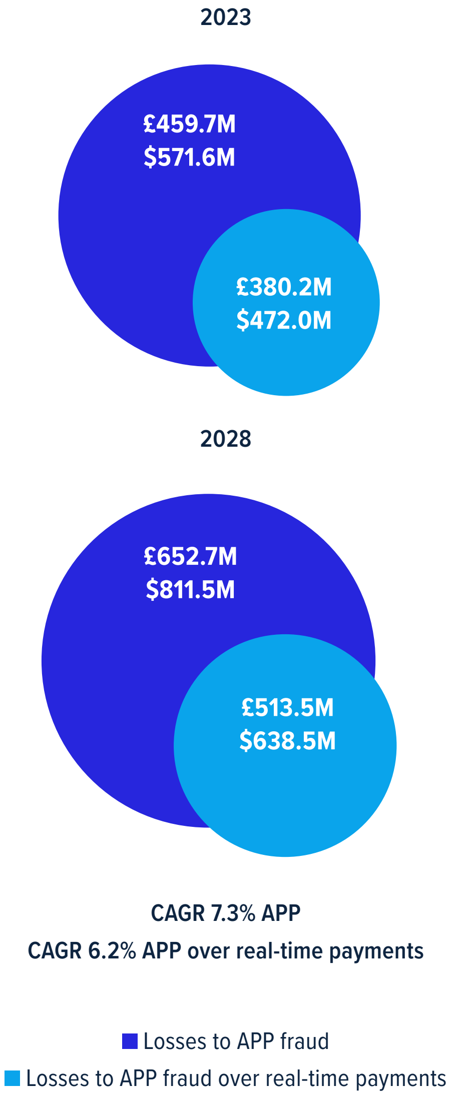
The rise of immediate payment systems in the U.K., while boosting convenience, has also seen an increase in APP fraud. With no time to reflect or cancel a transaction, consumers are often tricked into authorizing fraudulent payments.

The U.K. has uniquely adopted a 100% reimbursement approach

Compared to other countries, the U.K. has made significant strides in fraud victim protection. Many U.K. banks report reimbursing between 80% and 96% of scam victims, far outpacing other regions. This progress is largely driven by regulatory frameworks that enforce customer reimbursement for fraud losses, particularly in authorized fraud cases where banks are found negligent.

As part of the U.K.'s broader fraud strategy, the Payment Systems Regulator and the Bank of England are introducing a mandatory reimbursement scheme for victims of APP fraud. This new scheme, effective from October 2024, requires payment service providers to reimburse APP fraud victims within five working days, with costs split equally between the sending and receiving banks. Faster Payments Service and retail CHAPS payments are included, and special provisions apply to vulnerable consumers.

Growth of APP scams vs. APP scams over real-time payments

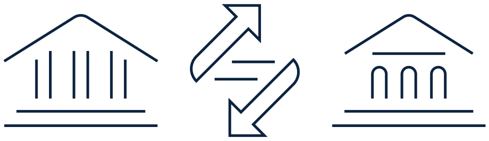


Country insight: U.K.

Introducing a 50/50 liability split between sending and receiving banks is one of the most significant moves globally for APP mandates

By mandating a shift in liability to both senders and receivers, U.K. banks will need to enhance their real-time monitoring of mule risk and incoming payments, leading to a more standardized approach.

This focus on exit accounts has the potential to not only disrupt criminal networks but also foster a deeper integration of fraud prevention and AML efforts, ultimately advancing the fight against financial crime. On the downside, concerns remain within the banking community about user complacency and increased first-party and friendly fraud.



Tackling fraud through AI and collaboration

Reimbursement will only ever be part of the solution – victims still suffer and the criminals still get the stolen money. A cross-sector approach is crucial, as is the sharing of actionable intelligence and the delivery of proactive disruptive measures and operations.

The U.K. banking sector is making increasing use of AI and cross-bank collaboration to combat APP fraud. AI technologies, such as facial recognition and device intelligence, are proving effective against impersonation attempts and fraud schemes.

Furthermore, U.K. banks are exploring ways to share risk signals and suspicious activity indicators between institutions without breaching privacy regulations, allowing for real-time detection of fraud across multiple banks. Intelligence sharing across both the private and public sector is also a vital tool in disrupting and preventing fraud, and there have been major recent legislative changes, such as the Economic Crime and Corporate Transparency Act.

Nearly every second victim succumbs to advance payments and purchase scams

26%	Advance payment scams
23%	Purchase scams
16%	Impersonation scams
8%	Invoice scams
8%	Romance scams
7%	Investment scams
7%	Other
5%	Authority scams

Country insight: U.K.

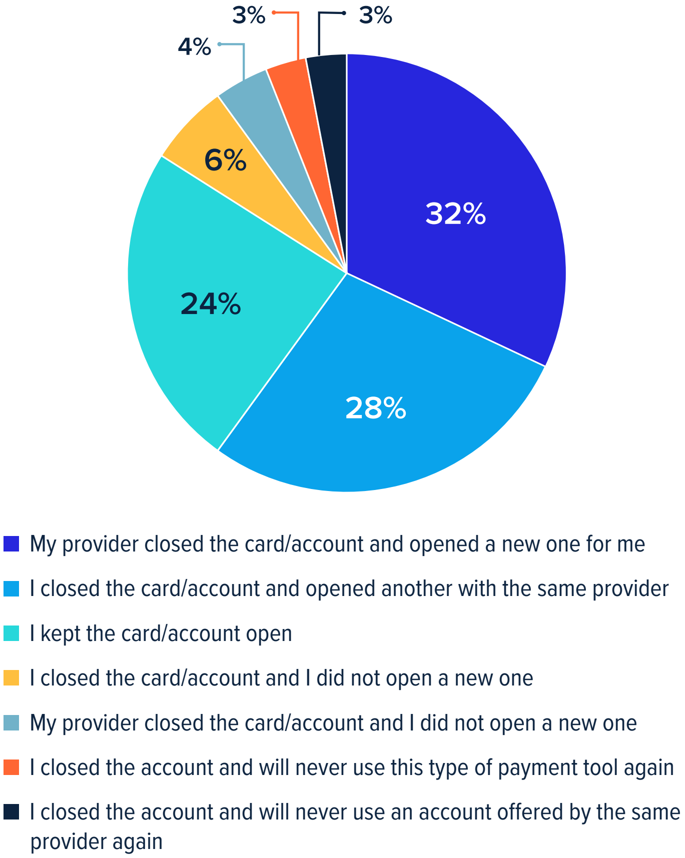
Future trends and the impact of economic conditions

Looking ahead, as fraud prevention measures tighten, the U.K. is likely to see an initial rise in first-party fraud cases as consumers feel more comfortable reporting fraud under the new reimbursement rules.

Economic factors such as the cost-of-living crisis may also drive an increase in fraudulent activity, as people facing financial hardship may be tempted to participate in scams. Fraudsters may turn to synthetic identity fraud or misuse legitimate accounts, making it essential for banks to enhance onboarding processes and guard against illicit account usage.

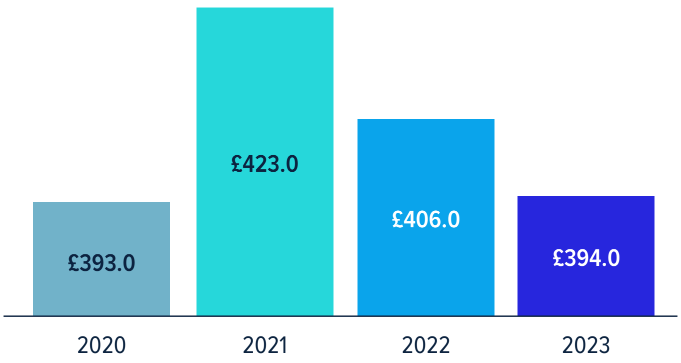
The move to make banks liable for compensating victims of APP scams is also fueling discussion about the role of social media companies in enabling scammers and whether they should also be accountable. This is prompting calls for tech firms to share more detailed intelligence on how criminals are abusing their platforms with retail banks in the U.K.

With stricter reimbursement measures, **the majority of the consumers chose to stay with their existing provider**, while 13% of the victims chose to end their relationship with their existing financial institution



Country insight: U.K.

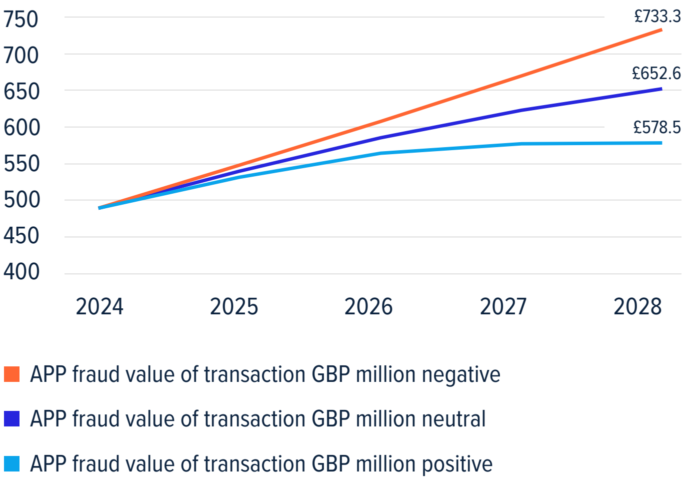
Average loss per scam (£)[2]



The average loss per case in the U.K. was £394.0 in 2023. This figure represents a return to the 2020 level, before a peak of £423.0 in 2021, possibly due to the COVID-19 pandemic. This change indicates a 7% slight decline from 2021 to 2023.

Forecasting the evolution of scams in the U.K.

Further investment could save U.K. banks $200 million in scam loss by 2028



With a CAGR of only 3.5% in the past five years, scam losses in the U.K. have been notably restrained compared to the U.S. and Australia. Public awareness of scams is high, both in the media and among survey respondents, indicating a relatively informed population. But the threat remains significant. Around 15% of scam victims surveyed either closed their affected accounts without reopening others or completely abandoned the service provider. This not only results in lost revenue but also carries considerable reputational risks for banks.

Looking ahead, the U.K. could face potential losses of up to $911 million by 2028 if economic conditions deteriorate and the industry fails to maintain its momentum in anti-scam measures. Conversely, under favorable conditions—particularly with increased investment in AI and continued initiatives like the recent AI summit—the U.K. could potentially save nearly $200 million in APP fraud losses by 2028.

Consumer survey base: 151 scam victims

Conclusion: The U.K.'s mandatory reimbursement regulation represents a bold step in protecting consumers from APP fraud. While the industry faces operational challenges, it is crucial for banks to maintain faith in the new system. By tightening onboarding processes and embracing real-time collaboration across FIs, the U.K. banking sector is well positioned to lead in the fight against scammers. Other regions will be closely monitoring progress and using U.K. outcomes to influence their own local policies.

[2] *Source: U.K. Finance*

Country insight: Australia

Market stopping short of mandates to tackle multifaceted scams

The financial impact of scams in Australia remains significant

Fraud losses in Australia have reached more than $3 billion[3] and have seen a staggering 80% increase year on year. Investment scams are particularly prevalent, with the Australian Financial Crimes Exchange reporting that they make up around one-third of total scams and an estimated $1.3 billion[3] in losses.

Scams involving fake merchant sites are becoming increasingly common, undermining consumer trust. This issue is particularly concerning for smaller merchants without established brand recognition, making them more vulnerable to these deceptive practices.

Other major types of scams include phishing, romance scams, and newer threats like payment redirection and fake bills. In the B2B sector, CEO fraud (where an invoice payment is requested by the “boss”) is a growing concern. Additionally, small businesses are being targeted with account takeovers as scammers issue invoices with different BSB/account numbers to existing customers – a good reason for introducing Confirmation of Payee.

Another worrying trend is that scammers are proactively targeting people with disabilities. Seasonal scams also frequently emerge, especially around tax time, when individuals are targeted with fraudulent tax-related messages.

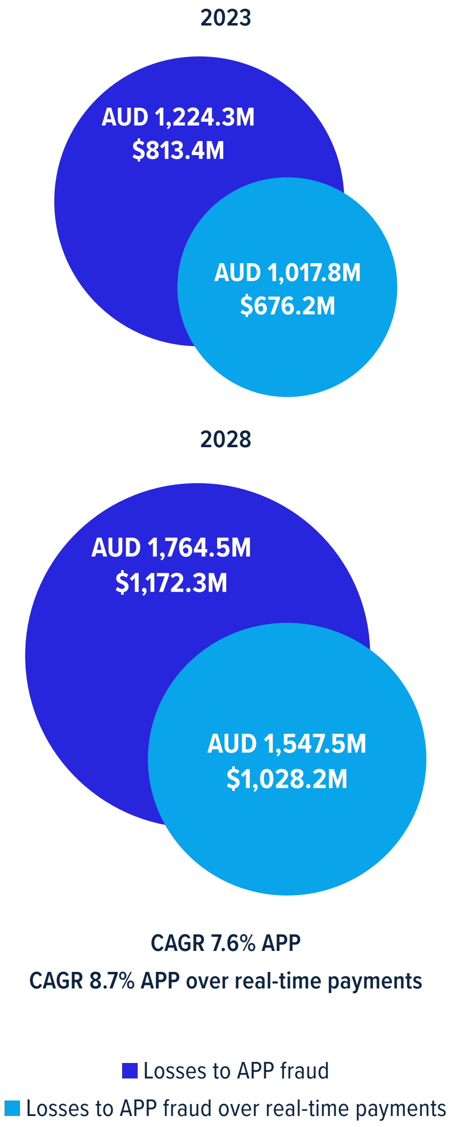
Industries are uniting in response to rising scam incidents

Approximately 65%[3] of Australians have encountered a scam attempt, highlighting the urgency for preventative measures.

Despite advancements in technology, such as the use of AI by both scammers and fraud detection systems, the effectiveness of prevention relies heavily on data sharing among FIs. A collaborative approach is essential to identify and mitigate scams proactively.

Australia launched its National Anti-Scam Center (NASC) in July 2023 to foster collaboration between banks, FIs, and telecommunications providers to combat scams effectively. Early signs indicate success, as many people are reporting fewer scam phone calls.

Growth of APP scams vs. APP scams over real-time payments



[3] *https://www.accc.gov.au/media-release/accc-calls-for-united-front-as-scammers-steal-over-3bn-from-australians*

Country insight: Australia

Focus on mule accounts

While awareness of scams is increasing, the challenge is far from resolved. As scammers refine their tactics, ongoing vigilance and cooperation across sectors will be necessary to maintain trust in the digital marketplace. It's crucial to emphasize that protecting consumers from scams goes beyond merely stopping the scam itself.

A significant part of the effort involves identifying and shutting down mule accounts and exit accounts, as the stolen funds need to be traced. Preventing banks from becoming unwitting participants in the scam chain is essential. The NASC has commenced a scam website takedown service targeting, among other things, phishing scams and online shopping scams. This is in addition to the Australian Securities and Investments Commission's takedown of investment scam websites.

Australia is looking to the U.K. for inspiration but stopping short of liability mandates

In August 2024, the Australia Banking Association announced that the country would adopt a similar solution to the U.K.'s Confirmation of Payee, which gives customers more confidence that they are transferring money to the right person and not to a potential scammer. It forms part of the sector's Scam-Safe Accord, which is a set of world-leading safeguards by banks to help keep the money of Australians safe.

Unlike the U.K., however, Australian banks aren't mandated to reimburse victims of scams. As discussions progress among banks and regulators, there is a possibility that may change. If banks fail to take adequate measures against scams, regulators may impose liabilities on them. Clear regulations are necessary to define consumer responsibility in cases of fraud, particularly in bank-to-bank transfers, whether in real time or otherwise.

Australia has also seen the introduction of a digital identity initiative, Connect ID. Although this has been adopted by several banks, there are concerns about mandating such a scheme, as customers of smaller banks may struggle to access their data through such solutions.

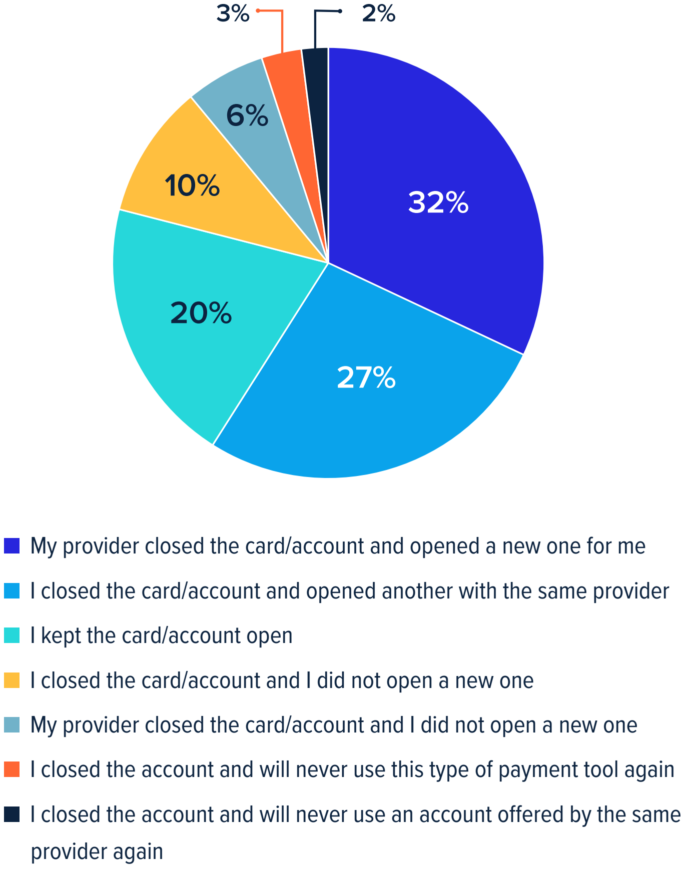
The Australian Treasury is actively developing a strategic plan that includes actions to investigate and enhance the fraud prevention landscape. However, most regulatory influence has been limited to recent years, with local associations like AusPayNet previously holding more sway over payments management.

More than half of victims have been subjected to a scam related to a product or a service, i.e., purchase, advance payments, and invoice scams

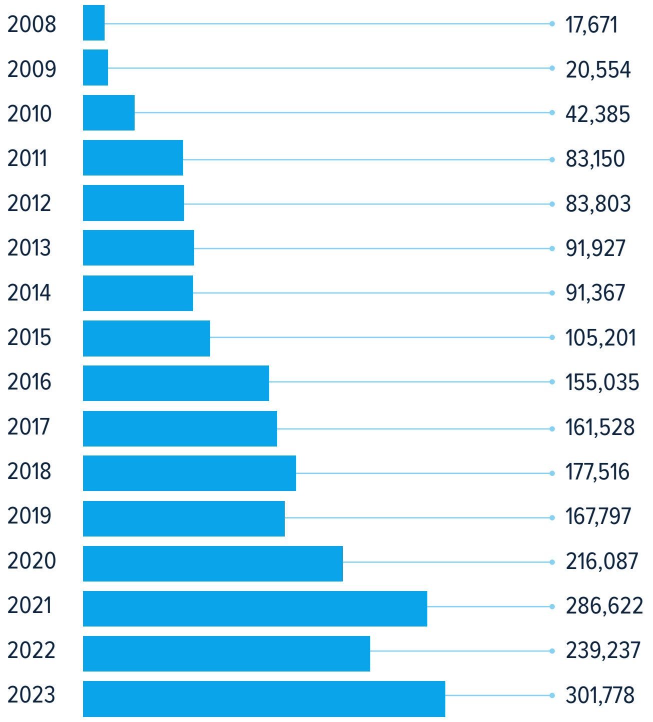
26% Purchase scams	**20%** Investment scams	**17%** Advance payment scams	**12%** Invoice scams
11% Impersonation scams	**6%** Authority scams	**5%** Romance scams	**3%** Other

Country insight: Australia

Inflicted by loss of consumer confidence, **1 in 5 consumers chose to move away** from the existing financial institution



Number of scams received by the Australian Competition and Consumer Commission



Source: Australian Competition and Consumer Commission (ACCC)

The ACCC received a record number of scam reports in 2023. This represents an explosive increase compared to the past decade, and even compared to 2021, which had the second-largest peak, similar to other countries analyzed.

Scams reported to all agencies in Australia in 2023 show an average value of AUD 4,500 considering the total loss and the number of reported scams. This value appears to be much higher than in the U.S. and the U.K., for example.

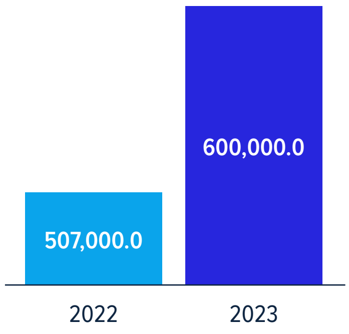
Fraud detection must embrace real-time intelligence sharing

Recent initiatives by Australian banks like Westpac have shown promise in moving from manual detection to digital solutions for identifying potential scams. Collaboration and data sharing must be reciprocal; currently, there are instances where banks receive data but do not reciprocate.

And the shift toward real-time payments brings both opportunities and risks. Although it allows for quicker transactions, it also presents a tempting target for scammers, especially if the associated limits are not strict enough to mitigate potential losses.

Country insight: Australia

Number of reported scams



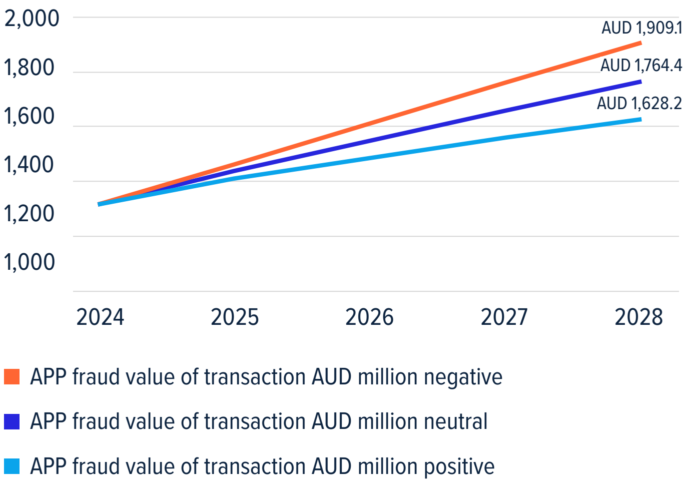
2023 stats

Total fraud loss
AUD 2.7B

Average fraud loss per case
AUD 4,500

Forecasting the evolution of scams in Australia

Scam growth has become a significant problem in Australia



APP fraud losses in Australia have surged dramatically over the past five years. With a CAGR of 39.6% from 2019 to 2024, it closely mirrors trends in India. Australia has made progress to address this issue, leading to a projected slowdown in growth over the next five years. Considering Australia's relatively underdeveloped status as a real-time payments market, more needs to be done, as the future hinges on its ability to get this issue under control.

In the most pessimistic scenario, if initial efforts to combat scams are not sustained and economic conditions worsen, Australia could face an additional $222 million in APP fraud losses over the next five years. Notably, more than 20% of scam victims in Australia choose to sever ties with the bank where the fraud occurred, indicating that the potential financial and reputational losses for Australian banks could be even more substantial.

Consumer survey base: 142 scam victims

Conclusion: Collaboration among banks and industry stakeholders in Australia is improving, as evidenced by initiatives like Scam Watch and recent data-sharing efforts that have successfully shut down numerous scams. By leveraging real-time signals and advanced data sharing, the industry can disrupt fraud more effectively. With many scams in Australia originating from countries like China and Russia, it raises the question of whether international collaboration is necessary to combat these frauds effectively.

Country insight: India

Countermeasures are making inroads in India but are they enough?

The Indian government's Digital Public Infrastructure program has propelled India's modernization, transforming it into the world's third-largest digitalized country. As more of its citizens make the leap online for banking, shopping, and social activities, they are increasingly exposed to APP threats.

Today, most of India's fraud currently happens in the digital space

Scammers are utilizing technology as a medium, focusing on socially engineered frauds, account takeovers, phishing, and cyclical trends. Common fraud types include triangulation, refund fraud, malware fraud, and romance scams that target specific age groups and geographical regions. A recent fraud trend involves impersonating law enforcement officers and tricking victims into transferring money to a false trading company by claiming their bank account was involved in money laundering.

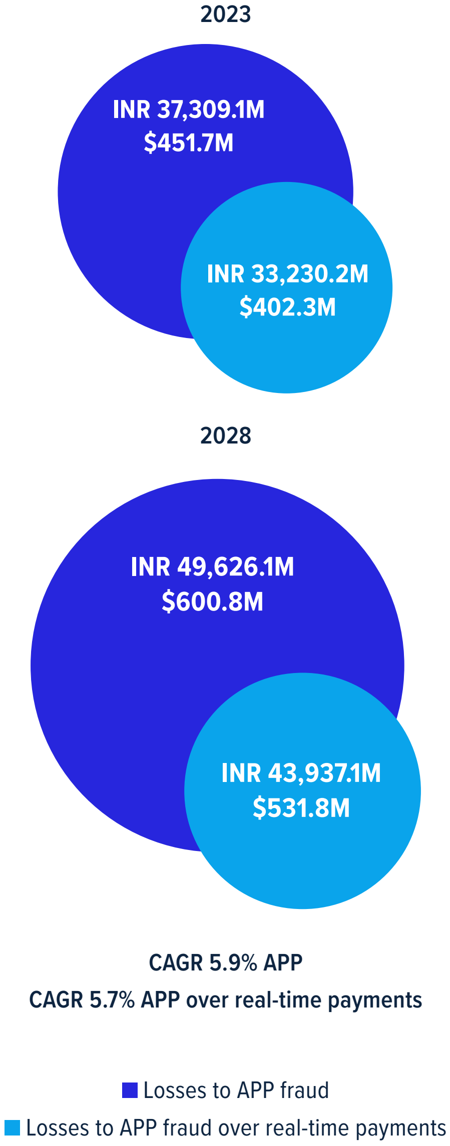
While cross-border scams from regions like Africa and the Philippines occur, domestic scams are more prevalent in India due to Indian fraudsters' tech skills and creativity in manipulating systems.

Positive countermeasures and victim support

To tackle these types of scams, the Reserve Bank of India (RBI) has initiated education programs advising people to verify claims with authorities before taking any action. However, reaching and educating the entire population is challenging due to India's linguistic diversity.

In India, most APP scams are driven by understanding of victim behavior rather than by using AI as a direct tactic. However, AI is now used extensively for account takeovers and sending bulk phishing messages. To counter this, India's banks are implementing profiling and transaction monitoring to detect synthetic identities and suspicious transactions. The RBI mandates banks compensate customers for negligence and penalizes banks for inadequate transaction monitoring.

Growth of APP scams vs. APP scams over real-time payments



Country insight: India

Faster payments demand faster scam detection and greater awareness

Fraudsters have been quick to exploit the success of India's Unified Payments Interface (UPI) platform, running in the slipstream of real-time payments to go under the radar.

Fake UPI apps attempt to mimic legitimate ones to steal user information or set up fake stores to receive payments for goods that will never be received. Banks are responding with measures like using micro-transfers for verification and profiling to detect suspicious UPI transactions. Additionally, the RBI has now mandated that banks and non-banking financial companies must implement early warning systems to detect fraud and scams, with minimal manual intervention and using AI.

Bridging the knowledge gap

It's clear that one of the biggest challenges in banks' defenses is the lack of consumer understanding, especially in rural and semi-urban areas where people may be more susceptible to fraud. While the awareness gap is diminishing, there are still specific types of fraud like synthetic fraud and socially engineered fraud happening across organizations. There is a need for better understanding of the payments domain, how to rectify issues, and how to better identify scams.

Improving transaction monitoring systems

While most banks use cutting-edge technology for transaction monitoring, only a small percentage do so effectively, leaving the majority vulnerable. The RBI is trying to ensure that every bank has a robust transaction monitoring system with advanced technologies like AI and customer profiling.

Banks in India are starting to collaborate with each other and with other entities like telecom companies and internet providers. There is a system being developed for sharing financial crime reports among banks so they can better understand various fraud methods and countermeasures. The RBI is also setting up an anti-fraud forum where banks can share information and best practices, with the State Bank of India taking the lead.

Banks must embrace AI to reduce internal vulnerabilities

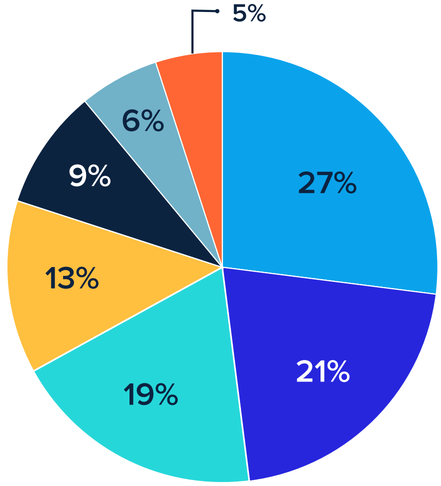
When it comes to scams, India's perpetrators are infinitely creative and tech savvy, and they can attack at scale. This makes it difficult to predict what's happening now—and to sidestep their next move—without the automated speed and accuracy of AI.

Impersonation scams are at large in India, coercing and intimidating individuals to transfer funds by creating a sense of urgency

21% Impersonation scams	**18%** Investment scams	**15%** Advance payment scams	**14%** Invoice scams
14% Authority scams	**11%** Purchase scams	**5%** Romance scams	**2%** Other

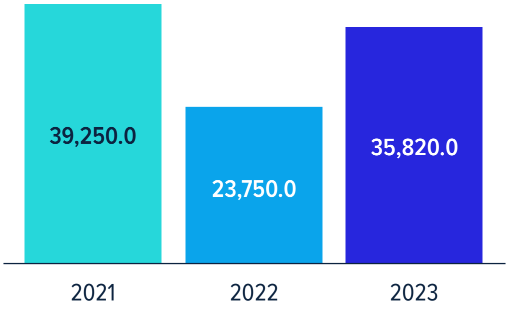
Country insight: India

Over one-third of the victims lost confidence in their existing financial institution and ended up moving away



- ■ I closed the card/account and opened another with the same provider
- ■ My provider closed the card/account and opened a new one for me
- ■ I kept the card/account open
- ■ I closed the card/account and I did not open a new one
- ■ I closed the account and will never use an account offered by the same provider again
- ■ My provider closed the card/account and I did not open a new one
- ■ I closed the account and will never use this type of payment tool again

Average loss per scam (INR)

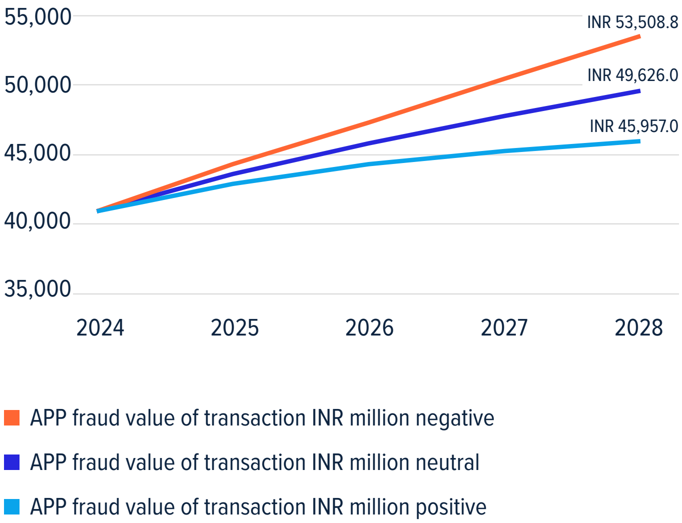


2023 experienced a 43% increase compared to 2022 in average scam values, as scammers shifted to more advanced phishing, impersonation, and UPI-related scams involving larger sums.

Country insight: India

Forecasting the evolution of scams in India

Knock-on effects of scams are highest in India

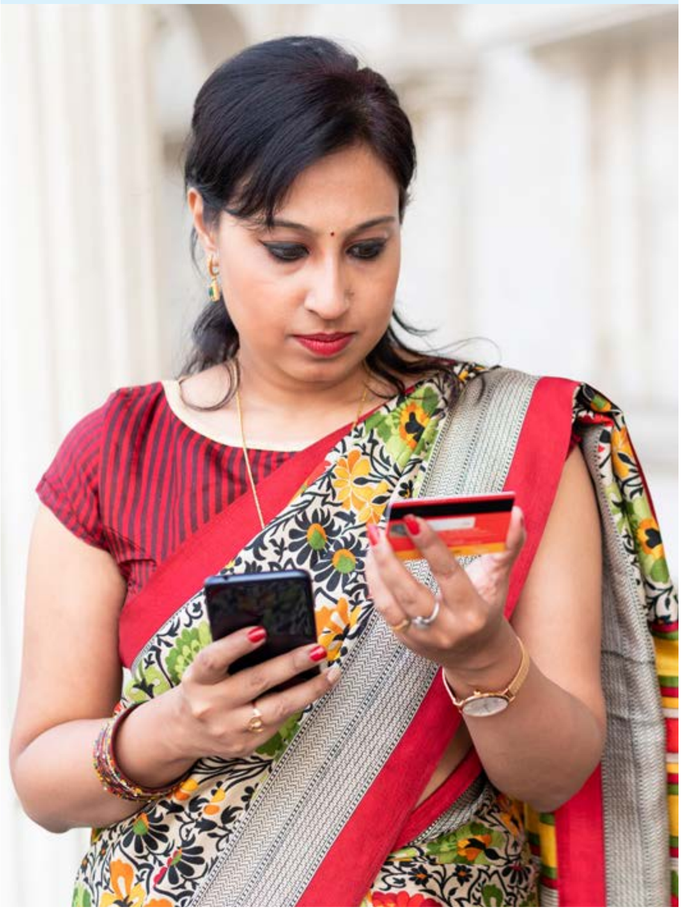


As the single most developed real-time payments market worldwide, India has seen a huge spike in APP and real-time fraud losses in the last five years. In 2024, however, fraud losses have dropped rapidly as countermeasures are brought to bear. Indeed, India is beginning to come to grips with the problem more effectively than any other market in the study, with the lowest forecast CAGR for APP fraud losses (6.0%, 2023-28).

However, there is no room for complacency. The risk of APP fraud in India is among the highest of any country included in this study. Furthermore, more than one-third of scam victims surveyed reported that they ceased doing business with their FI after experiencing fraud. This suggests that revenue and trust losses could far exceed the anticipated $600.8 billion in direct APP fraud losses by 2028. Under our most pessimistic forecasts, an additional $105.6 billion could be lost in the next five years unless proactive measures against APP fraud are implemented.

Consumer survey base: 199 scam victims

Conclusion: Indian banks are aware of new AI solutions and are using them to some extent, but there is still much room for enhancement in its adoption, particularly in areas like loan origination, credit risk analysis, and know your customer (KYC) processes. As with all countries where the emphasis has been on boosting financial inclusion, finding ways to identify and shut down mule and exit accounts without creating onboarding or transaction friction for legitimate users remains a fundamental hurdle that is proving difficult to cross using existing tools and resources.



Country insight: Brazil

Data sharing is now key to real-time risk reduction

PIX gangs are taking advantage of Brazil's mobile payments boom

Brazil's immediate payments scheme PIX has significantly enhanced convenience for consumers and businesses alike – but it has also opened a new avenue for fraudsters who seek to exploit the speed and ease of real-time payments for their own gain.

Through its central bank BACEN, the Brazilian government has implemented several measures to mitigate this threat, but the battle against financial fraud is still ongoing. A key challenge is that once funds are transferred through multiple real-time accounts, recovering them becomes nearly impossible.

In response, Brazilian financial authorities have introduced several measures aimed at preventing these crimes:

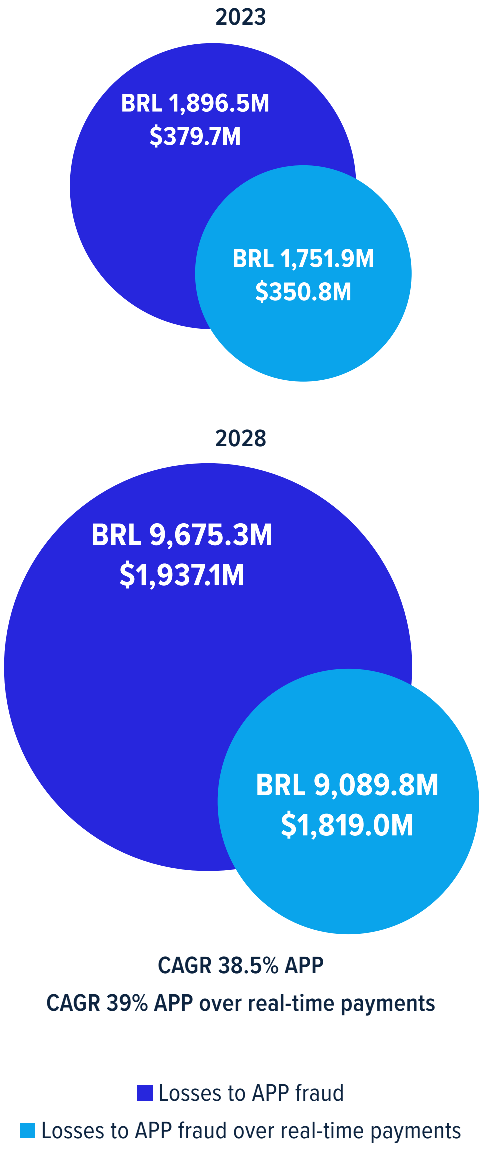
- **Transfer limits:** It now allows users to set caps on transfers, based on factors such as time of day and geographical location.
- **Behavioral monitoring and device verification:** FIs are integrating location-based and behavioral monitoring to flag unusual activity that might suggest fraudulent behavior.
- **Data sharing between institutions:** To enhance detection and prevention, banks are collaborating more closely, sharing transactional data while protecting customer privacy.

AI has become a double-edged sword

On one hand, the widescale availability of generative AI is making it easier for scammers to carry out more convincing impersonation attempts through voice calls and phishing emails and more sophisticated schemes. On the other hand, Brazilian banks are leveraging AI to bolster their own fraud detection systems.

From analyzing customer transactions to enhancing fraud prevention, AI is playing a growing role in spotting fraudulent activity, especially in real-time systems. However, the integration of AI for APP fraud remains an evolving space, and further collaboration across industries such as banks, telecoms, and internet providers is necessary to stay ahead of these ever-changing threats.

Growth of APP scams vs. APP scams over real-time payments



Country insight: Brazil

Scams that prey on people's familiarity with household bills are becoming more common in Brazil

Aside from product and investment scams, which have seen the highest growth, romance scams continue to be an issue – in some cases leading not only to financial loss but more serious consequences, like kidnapping. Another major shift is the rise of bill fraud, where scammers send what look like genuine payment requests from trusted companies, like mobile or television service providers. They often use fake discounts or urgent due dates to trick consumers into making spontaneous payments. This reinforces the critical role of consumer education to encourage individuals to "stop and think" before paying and to help them recognize suspicious requests and avoid becoming targets.

Legislative and regulatory action aims to increase data sharing

The Brazilian government, led by BACEN, has made regulatory moves to curb APP fraud. One major development is Resolution 6, which was introduced by BACEN and the National Monetary Council to improve fraud detection and reporting. Since November 2023, all FIs in Brazil are required to collect and share detailed information on fraud incidents. This includes:

- A description of the probable cause of the fraud or attempted fraud
- Information on the alleged perpetrator
- The recipient bank and account details involved in the fraudulent transaction

These measures aim to create a comprehensive database for monitoring fraud trends to identify perpetrators more efficiently and help track down mule accounts.

Three out of five victims are falling prey to product scams i.e., purchase, investment, and advance payment scams

22% Purchase scams

21% Investment scams

17% Advance payment scams

13% Invoice scams

9% Impersonation scams

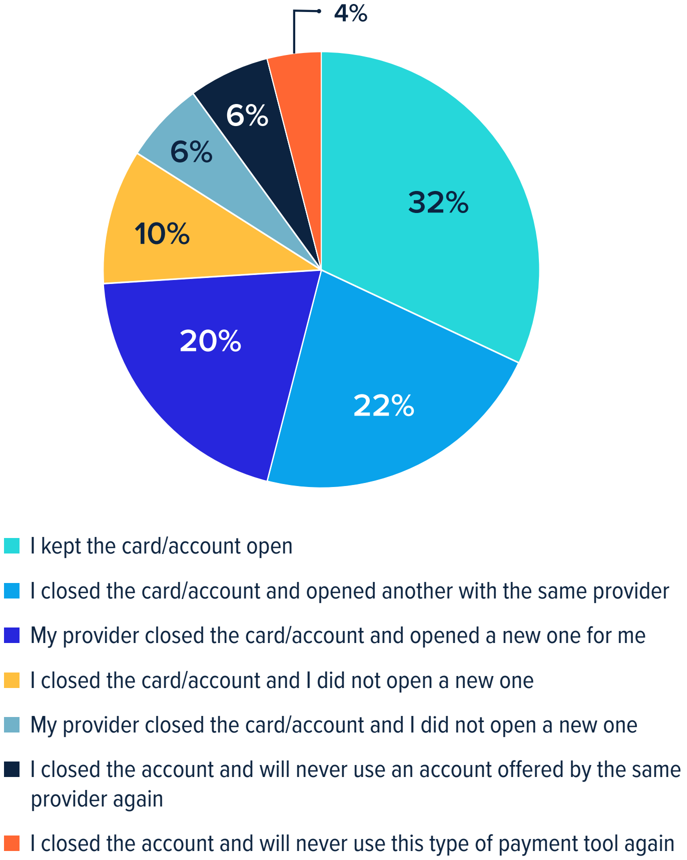
7% Authority scams

7% Other

4% Romance scams

Country insight: Brazil

One out of four victims chose to leave their existing financial institution



The role of education and awareness

According to Brazil's banking association, nearly one in three[4] Brazilians have been victims of financial scams.

Consumer education is now an essential element in the fight against APP fraud. Banks, regulators, and fintech companies are actively educating the public about the risks associated with digital payments, particularly real-time transfers through PIX. Public awareness campaigns aim to make users more vigilant, reducing the success rate of fraud attempts.

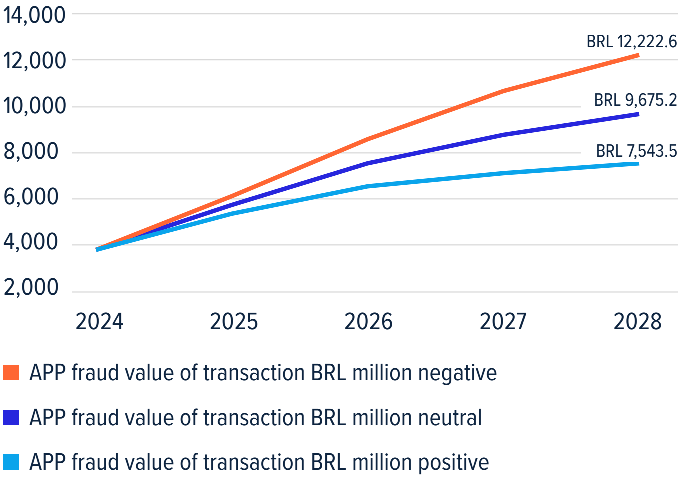
Open banking is thriving in Brazil, and there also needs to be more awareness of synthetic identity and monitoring of exit accounts from fintechs. The drive for frictionless financial inclusion has made it much easier for scammers to set up mule accounts. At the same time, they are also exploiting economic hardship and "buying" exit accounts from those struggling to make ends meet.

[4] *https://www.reuters.com/article/markets/feature-pix-gangs-cash-in-on-brazils-mobile-payments-boom-idU.S.L8N37Z4E1/*

Country insight: Brazil

Forecasting the evolution of scams in Brazil

Brazil stands to save more than $1 billion in scam losses 2024-2028



As the second-largest real-time payments market globally, Brazil faces a high risk of APP fraud, further complicated by the influence of organized crime. Our analysis indicates that by implementing advanced AI strategies, Brazil could potentially save more than $1 billion in fraud losses by 2028 However, without the timely adoption of effective anti-fraud solutions, it risks losing nearly $2.5 billion to fraud in 2028 alone.

The Brazilian banking industry is actively adopting various measures to combat APP fraud. But even under the most optimistic scenario, APP fraud is projected to grow at a CAGR of 31.8% from 2023 to 2028. Beyond financial loss, more than 25% of scam victims in the GlobalData survey indicated they would abandon the compromised account or provider. This poses a significant long-term risk to revenue and customer trust, which Brazilian banks must incorporate into their strategies.

Consumer survey base: 199 scam victims

Conclusion: While Brazil has made significant strides in tackling APP fraud, the battle is far from over. Real-time payment systems are a vital part of the modern economy, but they come with inherent risks that require constant monitoring and innovative solutions. BACEN's new regulatory framework, combined with greater industry collaboration and the use of cutting-edge technology like AI, offers a path forward. As scam tactics evolve, so too must the systems designed to protect Brazilian consumers.

Country insight: UAE

AI is making fakers harder to spot

Rising threats and increasing sophistication

The UAE is witnessing a rise in sophisticated scams, particularly investment scams and SMS-based card fraud. These schemes often originate from regions like East Africa, West Africa, and the Indian subcontinent. However, APP scams specifically tied to real-time payments have only recently emerged in the UAE due to the recent implementation of an immediate payments system.

Though APP scams are not as widespread in the Middle East as they are in Europe and the U.K., the landscape is changing. With real-time payment systems now in place, countries like the UAE are beginning to see a rise in familiar scam types—such as investment fraud, counterfeit goods schemes, and romance scams—though the scale remains smaller compared to other regions.

Cultural and regulatory influencers

Addressing fraud in the UAE presents unique challenges due to cultural and regulatory differences compared to regions like the U.K. and Europe. The lack of a standardized reimbursement model for fraud victims and varying government guidelines can make efforts more complex.

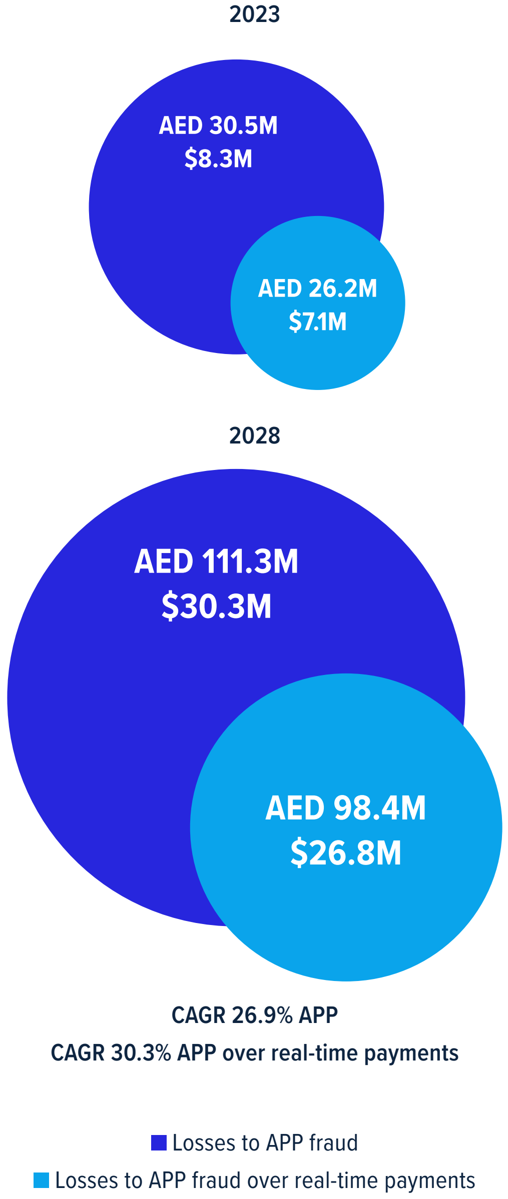
Additionally, cultural factors may discourage individuals from reporting scams, particularly in the absence of compensation or clear processes for recourse, which can result in challenges in gathering reliable data on the issue.

Digital identity and emerging fraud trends

Initiatives such as the UAE Pass digital identity system aim to enhance fraud prevention, but these systems still rely heavily on physical identification, limiting their effectiveness. Moreover, they do not adequately address scams initiated through texts, social media, or email.

The sophistication of fraudsters continues to evolve, with generative AI being used to create highly convincing deepfakes. One notable case involved a deepfake CEO scam that took place in the UAE last year.

Growth of APP scams vs. APP scams over real-time payments



CAGR 26.9% APP

CAGR 30.3% APP over real-time payments

Country insight: UAE

AI-driven malicious activities

AI is becoming a popular tool for scammers, enabling them to generate malicious code and carry out fraudulent activities with increasing ease. Criminals have an edge over organizations as they are not bound by regulatory constraints, allowing them to use AI for malicious purposes. The improved quality of AI-generated content, often indistinguishable from native English speakers, makes it harder for victims to detect scams. This poses significant challenges for phishing and other fraudulent schemes.

Issues with cross-border scams and data sovereignty

The UAE faces a high prevalence of cross-border scams orchestrated by international criminal organizations. However, strict data sovereignty laws in the Middle East present challenges in sharing fraud-related intelligence across borders. This hampers efforts to leverage global data pools that could help identify and combat cross-border fraud activities.

The need for an indemnity process and consumer protection

Having an indemnity process can be considered as part of best practice against scams, so it is likely to be a key consideration as the UAE banking market matures.

Shifting liability from consumers to banks encourages FIs to invest more in fraud prevention technologies and strategies. Protecting consumers and ensuring trust in the UAE banking system is critical, especially as the region moves toward a more cashless society powered by digital payments.

That said, issues around distinguishing scams remain, with grey areas around complicity making it difficult for the banking sector to have consistent policies on how cases should be managed.

ACI's role in combating fraud in the Middle East

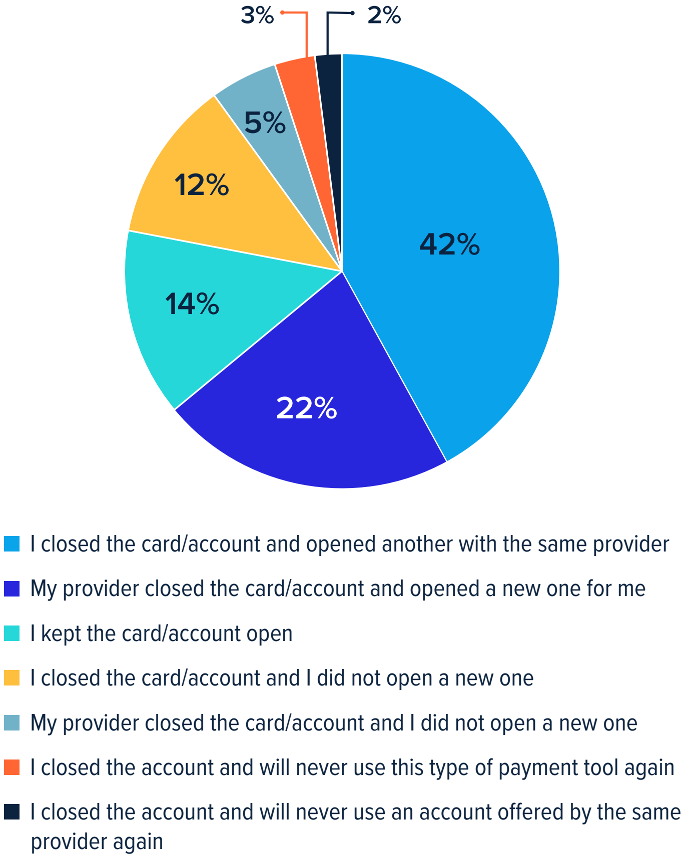
ACI has found success in the Middle East market not only due to its advanced technology but also because of its global experience in fraud prevention. ACI emphasizes a multi-layered approach – educating consumers, using cutting-edge technology, and prioritizing the customer experience. This approach continues to attract FIs in the region that need expert guidance and effective solutions to tackle fraud.

More than one in four consumers fall prey to investment scams and nearly one in five are victims of advance payment scams

29% Investment scams	**17%** Advance payment scams	**15%** Purchase scams	**15%** Impersonation scams
9% Authority scams	**7%** Invoice scams	**6%** Romance scams	**2%** Other

Country insight: UAE

As scams accelerate, **one in five consumers chose to end their relationship** with the existing financial institutions—directly impacting trust and confidence



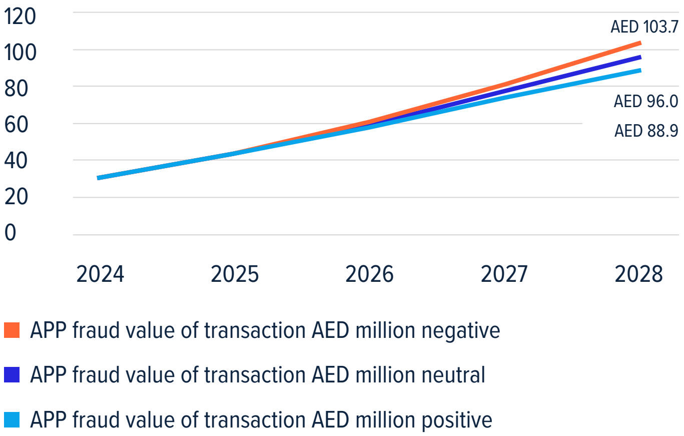
Implementing payments intelligence technology

ACI has already integrated its payments intelligence technology into the central infrastructure of some Middle Eastern countries, enabling banks within the network to share payments intelligence. This allows for real-time monitoring of incoming and outgoing transactions while keeping sensitive data localized within the country. This approach is expected to gain further traction as more nations adopt this centralized fraud prevention model.

Country insight: UAE

Forecasting the evolution of scams in the UAE

Losses are limited, but banks can’t ignore the risk of losing customers

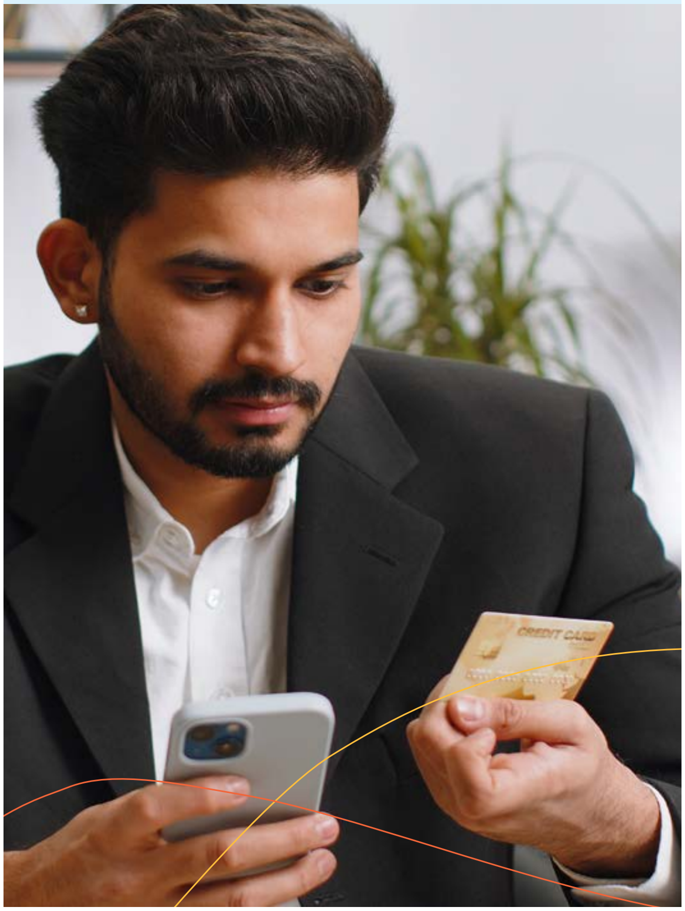


The UAE is the one of the smallest and least-developed real-time payments markets in this study. Its current AI strategy prioritizes growth and operational efficiency rather than directly tackling APP fraud. Due to its limited scale in real-time payments, APP fraud remains relatively low.

However, banks in the UAE should not overlook the broader implications of fraud. According to GlobalData’s survey, 22% of scam victims reported closing their accounts and switching providers after experiencing fraud. This trend poses a significant risk to both revenue and customer trust for FIs in the market.

Consumer survey base: 168 scam victims

Conclusion: The rise of APP scams in the UAE, driven by real-time payments and AI-powered fraud, poses new challenges for FIs, consumers, and regulators. A more unified approach—strengthening digital identity verification, enhancing data sharing, and using advanced payments intelligence—can better protect consumers. Continuing efforts to improve education and cross-border collaboration will also help the UAE to reduce financial losses and restore public trust as it moves toward a digital, cashless economy.



2024 Scamscope

Key takeaways

1

Scam losses are escalating, but positive action can reduce costs and rebuild trust

This year's report highlights the growing financial burden of APP fraud across various countries and the significant losses banks can expect to face if they don't act. It also underscores the millions of dollars of potential savings that could be achieved by leveraging advanced technology, including AI. The 2024 consumer survey reveals that scammers not only steal money but also drive victims to abandon their banks. This loss of customer loyalty can severely undermine consumer confidence and hinder efforts toward financial inclusion. Fighting scams is now about more than just protecting customers – it's crucial for reinforcing trust in the financial ecosystem.

2

Institutions must work harder to mitigate real-time risk and safeguard reputations

As markets embrace the advantages of real-time payments, the swift movement of funds also heightens fraud risks. This year's report shows that scammers are actively targeting real-time payments and that customers are dropping their banks based on their experiences of scams. To protect real-time rails and their reputations, FIs need AI-based, automated systems that can work quickly to detect and block fraudulent transactions. By leveraging real-time predictive intelligence, immediate payments can be made even safer, allowing for their continued growth without sacrificing security.

3

Scammers know no boundaries, so fraud fighters must democratize intelligence to remove theirs

Countries like Brazil and organizations such as the U.S. Federal Trade Commission illustrate that data democratization in fraud prevention is a transformative movement, not a fleeting trend. The same philosophy must apply internally between KYC and anti-fraud teams to dismantle mule accounts. By fostering collaboration and sharing information safely inside and across institutions, companies like ACI are leading the way in reducing silos, uniting efforts, and safeguarding consumers and institutions alike.

4

Regulators are pushing for collaboration and accountability

Governments and regulators worldwide are increasingly aware of the harmful effects of scams. In response, numerous cross-industry working groups have formed to tackle scams collaboratively. They are actively looking at how to best support victims of unauthorized fraud, and whether to enforce advanced controls for inbound and outbound funds movement. In the U.K., a liability shift now holds recipient banks jointly accountable for compensating APP scam victims, a pivotal move that could help dismantle mule accounts. While FIs have existing fraud systems, the emergence of new mandates underscores the urgency to leverage global and regional expertise to ensure compliance and protect their payment ecosystems.

Our commitment to fighting fraud together

As a partner to leading institutions, we believe that it is our responsibility to ensure transparency around complex threats and trends including fraud. The annual Scamscope report is part of this commitment.

Now in its third year, this report aims to provide an overview of the scale and nature of authorized push payment (APP) scams in key markets to help support banks, governments, and legislators as they seek to mitigate risk.

This year's Scamscope highlights the escalating issue of APP scams and the urgency to protect consumer trust

The rise of AI as a tool for scammers—combined with the growth of real-time payments and the increasing use of digital channels for billing, social interactions, purchasing, and investment—has accelerated the pace of APP scams. These attacks can profoundly impact consumer relationships with their banks, eroding trust in individuals, authorities, and institutions.

Scam incidents are becoming not only more frequent but also more costly

Banks face mounting pressure from governments and consumer organizations to address these issues. While many scams originate online or through phone calls, it is ultimately banks—not telecom, social media, or marketplace companies—that are expected to reimburse victims. Furthermore, banks are increasingly scrutinized for identifying recipient accounts used as "mules" in fraud and money laundering.

Fraud fighters are having to work harder to tackle increasingly diverse and sophisticated scams

Our 2024 report emphasizes that banks must prioritize the following actions:

1. **Enhance collaboration:**
   Financial institutions (FI) should break down internal silos and adopt cross-industry approaches to exchange intelligence and combat fraud more effectively.
2. **Invest in artificial intelligence (AI) and machine learning:**
   Leveraging AI for real-time analysis of transactional data is crucial for anticipating and preventing APP fraud without compromising consumer relationships.
3. **Focus on receiving accounts:**
   There is an urgent need to target the receiving end of payments, as fraudsters exploit "mule" accounts to access stolen funds.
4. **Meet evolving regulations:**
   Stricter regulations are emerging, holding banks accountable for scam-related losses and necessitating more sophisticated monitoring systems.

These developments call for a smarter approach to tackling APP scams

At ACI, we are committed to facilitating this evolution. As a key player in the global payments ecosystem, ACI proactively helps banks and FIs correlate the relationship between data, human, and artificial intelligence to effectively prevent fraud and manage risk. Our ability to flag potential risks with precision is augmented by our unique presence across the payments value chain and nearly 30 years of expertise in implementing AI-enabled solutions.

We are already implementing cross-bank fraud detection collaboration and assisting banks in adapting to regulatory changes while leveraging data and technology. While investing in technology is essential, collaboration is equally vital in the fight against fraud and scams. The newest generation of AI is built for purpose, preserving all data privacy concerns and enabling intelligence exchange at a machine learning level, enabling peers to learn "together" in real time and act against threats.

One of the themes emerging from this year's report is the need to democratize intelligence

At ACI we are working hard to empower fraud intelligence exchange. Using a new generation of multilayered, responsible AI tools, we are helping to deliver precise and real-time decision-making, enabling users to identify fraud efficiently. By sharing signals across institutions and adopting a collaborative approach, banks can outsmart fraudsters and protect their customers, ultimately fostering a safer financial ecosystem for all.

The report is just one of the ways we are uniting the industry, giving them the insight they need to tackle complex fraud challenges, protect customers, and build confidence while restoring trust.

Annett van de Bunt
Head of Marketing
ACI Worldwide

Analyst insight

Education alone will not defeat scammers

Despite a slowing in growth rate, APP fraud will continue to rise in the next five years. Indeed, many markets will continue to experience double-digit compound annual growth in scams over real-time payment rails up to 2028.

The ever-evolving nature of APP fraud

Fraudsters are employing various methods to carry out APP fraud, almost always using some form of deception to trick victims. They might pose as legitimate websites, apps, brokers, businesses, government departments, or individuals. The industry must urgently address these vulnerabilities, and while it has done well with card fraud, where a single bank was in full control of the strategies, APP scams require an initiating and a receiving institution to work together.

Regulators are hoping to spur banks into doing this through legislation that requires them to educate, inform, and, in some cases, to reimburse victims. However, simply closing gaps in fraud capability and mandating change won't suffice.

APP fraud differs significantly from other types of payments fraud; it relies much more on human behavior and cannot be resolved solely through technical standards and solutions. The tactics of fraudsters constantly evolve, becoming more acute due to faster transactions and the growing number of individuals attempting fraud, driven by economic pressures.

Challenges demand a new approach to fraud prevention

As more payments transition to real-time rails, banks must balance fraud prevention measures with maintaining customer access and protecting their reputations. Fraudsters continue to operate across borders, necessitating international collaboration and information sharing among FIs and authorities. However, achieving such collaboration proves challenging due to competing interests, regulatory differences, and data privacy concerns.

In efforts to clamp down on mule accounts, banks face tension between their fraud departments, which aim to reduce losses, and their accounts departments, which strive to generate revenue by making account openings frictionless. This conflict creates challenges in implementing stricter fraud prevention measures.

AI can help banks adapt faster

FIs need automated systems that can quickly detect and block fraudulent transactions in real time. Because APP fraudsters constantly adapt their tactics, banks require systems that can adapt continuously to identify ever-evolving scams.

AI solutions stand out as the optimal choice, delivering the speed, automation, and intelligence necessary to outsmart scammers. However, banks still approach AI implementation cautiously due to a lack of clarity about regulatory allowances and their inherent conservatism regarding consumer accounts.

The cost of failing to optimize AI strategies

Although the challenges of fraud are universal, this study shows that country approaches are far from uniform and are compounded by factors such as the adoption and maturity of real-time payments, with more advanced markets like Brazil and India facing greater threats.

When determining the financial savings associated with introducing more advanced AI strategies to combat fraud, our findings suggest that Brazil, with its highly developed PIX real-time payments market, could save more than $1 billion in fraud losses, but its slow AI development is hindering progress.

In contrast, India, which has had an effective AI strategy since 2018, already faces lower fraud losses, with potential savings only about one-tenth of Brazil's. The UAE is one of the smallest and least-developed real-time payments markets in this study and experiences the lowest real-time payment fraud losses and minimal savings potential ($6.2 million). Its AI adoption is focused on growth rather than fraud prevention.

Among the more economically developed markets like the U.K., U.S., and Australia, real-time payments usage is low, but APP fraud losses vary. The U.S. and Australia have seen rapid fraud growth (27.8% and 39.6% compound annual growth rate [CAGR] from 2018-2023, respectively), while the U.K.'s growth is only 3.5%. All three markets are investing in anti-fraud measures, with the U.K. showing leadership through regulatory updates and AI initiatives.

That said, the U.S. and Australia are being much more cautious in their adoption of AI. Taking a pessimistic outlook, this could lead to significant additional losses—estimated at $388 million for the U.S. and $222 million for Australia over the next five years.

A more holistic approach is necessary

It's clearly time for the industry to adopt a more holistic and unified strategy in combating APP fraud. A collective effort that integrates mandates, technology, collaboration, and education is the only way to effectively address the complexities of APP fraud and restore trust in financial systems.

To achieve this requires connected intelligence and a coherent approach to the use of AI—and that can only be realized by the democratization of fraud intelligence and a united approach by all those whose platforms scammers are currently exploiting. Until then, banks will have to lead the way.

Samuel Murrant
Consulting Director,
Financial Services
GlobalData

2024 Scamscope

Methodology

APP fraud and real-time payments fraud data is based on a core methodology of secondary research focusing on publicly available sources such as central banks, payment associations, company reports, and news feeds. Primary research was conducted where secondary information was unavailable or sparse. This consists of expert interviews and a consumer survey. The final data is produced via a triangulation of GlobalData's existing in-house datasets, information obtained from above sources (primary and secondary) and our analysis of the market.

These numbers are then further cross-checked using both a top-down and bottom-up approach to ensure reliability of the data. The data for each country was validated on various parameters, considering their digital payments landscape, instant payments size, payments fraud (including instant payments fraud and bank transfer fraud). By using this meticulous modeling technique, we ensure that our market sizing data is comprehensive and provides an accurate representation of the industry.

To the historic and current-year data derived from this methodology, we apply our proprietary forecasting model. The data generated from these models are then reviewed and finalized by our team of expert analysts.

To generate the scenario forecasts in the model, we have created a deviation of the macro-economic outlook based on the historic trend of the parameter. This trend then was carried on forward to create an outlook that is different from the baseline. If the trend was above the baseline—the scenario was positive, if below it was negative. We created a respective negative/positive scenario by mirroring the difference between a created trend and the baseline. This way we have created a positive/negative region for the scenarios. These assumptions were then passed onto the fraud data to study the impact and create positive/negative scenarios for the fraud data.

AI adoption parameters are reflected through the economic assumptions, correlating economic conditions with greater or lesser investment in AI technology. The countries were treated equally from the parameter selection perspective. This is to allow direct comparison. However, we understand that different countries can react differently to the same parameter; this was addressed by having unique parameter weights for each country. The weights were selected based on the strength of correlation between the parameter data and fraud data for each country.

About GlobalData

GlobalData is a leading provider of data, insights and analysis for the world's argest industries, covering 17 industry verticals including banking and payments. GlobalData's industry-leading data rests on a foundation of "Gold Standard" data derived from trusted central sources and a team of expert analysts in each sector.

About ACI Worldwide

ACI Worldwide, an original innovator in global payments technology, delivers transformative software solutions that power intelligent payments orchestration in real time so banks, billers, and merchants can drive growth, while continuously modernizing their payment infrastructures, simply and securely. With nearly 50 years of trusted payments expertise, we combine our global footprint with a local presence to offer enhanced payment experiences to stay ahead of constantly changing payment challenges and opportunities.

LEARN MORE

www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com
Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393