December 2023

# Scamscope

## APP scam trends in the U.S., U.K., India, Brazil, Australia and Saudi Arabia

A report by ACI Worldwide and GlobalData

ACI Worldwide®
Real-Time Payments

GlobalData.

# Table of Contents



# Introduction
## Shut Down Mules, Stop the Scammers

The criminals behind authorized push payment (APP) scams are only interested in one thing: monetary gains.

Over the years, limits on ATM withdrawals, 3D Secure and device-level biometric authentications have made it harder to convert fraudulent schemes into cash. Today, however, real-time payment rails offer the tempting prospect of immediate access to stolen funds. All a scammer needs to do is socially engineer (or trick) a consumer into sending a payment to a mule account they control before quickly transferring the funds somewhere untraceable, such as converting to crypto.

These scams are incredibly difficult for banks to spot and prevent in real time, given the initial payment is authorized by genuine users on their own device. But without ready access to mules, cash is harder to extract for scammers, and the business case becomes harder to sustain. That means the industry's best shot at controlling APP scams lies in disrupting mule accounts.

## Inbound payments intelligence is vital

Scammers often recruit mules with job offers such as "money transfer agent" or "payment processing agent," just as often they open or buy accounts based on fake or synthetic identities, a problem exacerbated by the influx into banking and payments of smaller players with less mature Know Your Customer (KYC) controls. A mule account might also be the result of an account takeover.

Regardless of their origins, mule accounts are able to go undetected because of the routine lack of monitoring of incoming payments at most banks. This makes it hard to effectively monitor for potential mule accounts and manage associated risks.

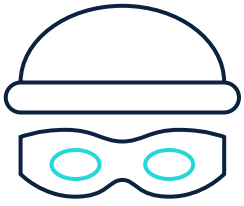
Therefore, the relatively simple step of monitoring incoming transfers — which existing anti-money laundering (AML) systems can handle — and whether they are quickly followed by transfers out, perhaps to crypto exchanges, would allow banks to start gathering some basic but vital intelligence needed to identify possible mule accounts.

## The regulatory battle to come

This intelligence would help prepare banks for incoming regulatory changes around scams.

Defining accountability and apportioning liability is a major challenge for the industry today. Banks might hold consumers accountable — after all, they initiated the transaction — but governments and consumers don't agree. Regulators are starting to pressure banks to invest in better controls to protect consumers. And the research in this report shows that plenty of scam victims walk away from their banks as a result of their experience.

If, as many commentators expect, regulators adopt shared accountability models similar to those being introduced in the U.K., intelligence on suspected mule accounts could limit banks' exposure to liability. In a regulatory scenario where sending and receiving ends share liability on a sliding scale, depending on the controls they have in place, banks that warn against making payments to suspected mule accounts can argue they did all they reasonably could to prevent the scam.



## Industry must get better at sharing information

This brings us to another major challenge in the fight against scams: the lack of a framework for effective and efficient information sharing between financial institutions.

Regulators are also increasing pressure on financial institutions to share more data as part of efforts to define and drive accountability for scams. Instead of persisting with more established — but proven to fail — modes of collaboration, such as consortium-led data models based on industry-wide fraud insights, a network intelligence model that empowers the two ends of transactions to collaborate directly would be more effective. By exchanging signals rather than data for use in federated machine learning models, financial institutions could collaborate in real time to profile the risks related to transactions, without compromising IP, data privacy or compliance obligations.

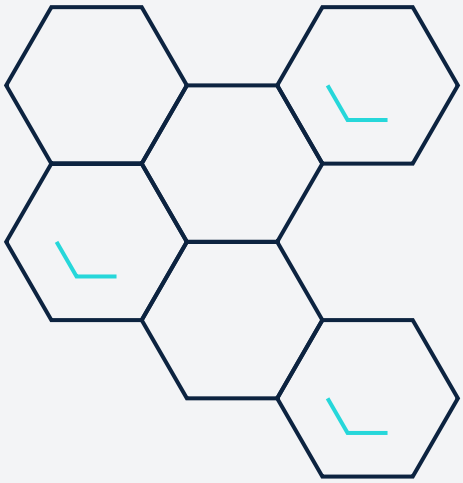
This intelligence-sharing network could also be expanded to encompass the big tech players that are party to scams. As banks have pointed out to regulators, these platforms certainly have a degree of accountability: Many scams originate on social networks and messaging platforms in the form of phishing, phoney ads or longer-running manipulations, such as romance scams. Their intelligence would be invaluable, and better controls on who is on those networks and what they're able to advertise would make scams infinitely harder to get off the ground.

## We have the tools

Financial institutions, regulators and vendors already have the technology and know-how needed to identify mule accounts and share fraud signals, which would enable a more nuanced approach to accountability. The same AML and KYC technologies and processes that monitor inbound transactions can also monitor outbound payments. Network intelligence solutions are already available. And ISO 20022 opens a data path for exchanging vital fraud signals.

In other words, the industry has all the tools it needs to make real-time rails the most trusted and secure payment rails available — it just needs to perfect their use.

**Cleber Martins**
Head of Payments Intelligence & Risk Solutions
ACI Worldwide



Analyst Note

# Consumer Education and AI Are Key To Containing Scams

Losses to APP scams are expected to record an average compound annual growth rate (CAGR) of 11% from 2022 to 2027 across our studied markets (U.K., U.S., India, Brazil, Australia and Saudi Arabia), reaching a total of US $6.8 billion.

However, during the same period, the overall value of real-time transactions is also forecasted to grow, and at a faster pace, reaching 25% CAGR.

While this means that proportionally, the financial impacts of APP fraud become less of a problem for banks, it should not be mistaken as a reason to rest on their laurels. Rather, it illustrates that the window of opportunity to get out ahead of the issue remains very much open.

For now, at least. Because with mounting losses impacting consumers and the increasing importance of real-time payments to national economies, most markets seem to be trending towards regulators obliging financial institutions to reimburse scam victims. At the same time, our research reveals trust implications for banks that could also cost banks dearly. Of survey respondents that report being a victim of fraud, around three in 10 close their accounts, meaning banks risk losing those relationships.

## Two solutions for banks to consider

Two items that have to be high on any banks' list of potential solutions to scams must be increased consumer education and boosting their own prevention capabilities through smarter technology.

APP scams are founded in social engineering, often originating on social media that targets the weak human link in a chain of strong technological defenses. Thus, a well-informed customer who knows how to spot a scam would be a powerful defense that banks should double down on building up. Anecdotal and isolated media reports of scams don't appear to be resonating in the public consciousness as things that they themselves should also be on the lookout for; respondents are still primarily concerned with the security of their card details online and with ways their card or card number can be stolen in shops or at ATMs.

On the technology front, there are strong hopes in the industry that AI can deliver on its promise as a transformative solution for scam detection and prevention. By helping banks to recognize more sophisticated patterns within their data, faster, AI should allow for better fraud prevention rates, fewer false positives and more proactive identification. It may also enable warnings to consumers in real time when risky patterns of behavior are detected.

## A complex challenge with room to grow

Banks' efforts to encourage regulators to hold social media platforms accountable for their role in scams means the debate is converging with wider challenges around misinformation. This illustrates the complexity of the problem and how social issues contribute to creating fertile ground for scams.

Similarly, it's not unreasonable to expect that global economic challenges will also make the general population more vulnerable to scams. The prospect of a one-time, high-return investment opportunity, or a too-good-to-be-true deal on products, becomes more attractive when your financial situation is more precarious or your faith in traditional investment assets is low.

Of course, solving these issues is beyond the direct reach of the banking industry. But they serve to demonstrate the challenging environment it finds itself in and further illustrate the value of getting out ahead of scams now.

**Sam Murrant**
Consulting Director (FS)
GlobalData Plc

# Executive Summary
## Global Overview and Key Takeaways

### Payments intelligence and seamless collaboration are key to getting ahead of scams

The increasing sophistication of social engineering, the key role of mule accounts in making scams profitable and industry wranglings over liability all make seamless collaboration between financial institutions essential. It is easier to identify mule accounts and behavioral anomalies that are indicative of scams if you are monitoring payments coming in and out, and if you have 360-degree visibility of the behaviors of accounts on both sides of a transaction. And bringing about this new era of payments intelligence demands the creation of an industry-wide network and process for sharing anonymized data signals to strengthen the insights available for automated AI systems.

### Get ahead of the regulators

Regulators are under pressure to resolve major questions around consumer compensation and institutional liability for APP scams, given both the growing number of consumers being impacted and the need to preserve trust in new payment networks. Current rules governing liability vary from region to region, but regulators are closely watching the U.K., where new rules mandate that the institutions at the receiving and initiating ends of transactions share the costs of reimbursing victims. It is reasonable to expect the lessons learned here will influence regulatory responses elsewhere.

### Disrupt mule accounts to break the chain

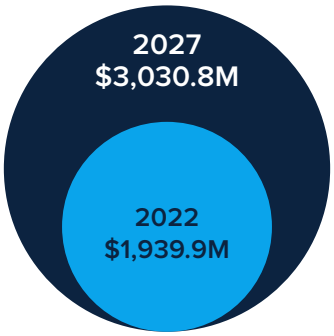
Mule account networks are a key aspect of the “business case” for scammers, allowing them to quickly move stolen funds beyond the reach of banks and the authorities. By making the relatively simple change of monitoring inward transactions rather than solely focusing on outgoing funds, banks are able to take a big step towards disrupting mule account networks and therefore breaking the chain of scams. With appropriate KYC in place, monitoring of money coming into, as well as out of customers’ accounts and analyzing the behavior of those accounts, banks could better monitor for mule accounts either held by synthetic or stolen identities, or instances where accounts have been taken over.

### Understanding the critical role of responsible AI

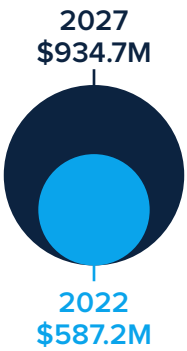
Machine learning has long been adopted by banks and financial institutions to understand and learn scam techniques and protect their customers. As the financial world moves into the era of artificial intelligence, it is critical to be proactive rather than prescriptive in the approach to combat scammers. By using multitudes of data signals and leveraging advanced technologies like voice biometrics, institutions can not only better understand their customers and their intent, but also make sure that emerging AI-fueled threats can be prevented without disrupting their customer relations.

## APP Fraud Value

U.S.




U.K.




India

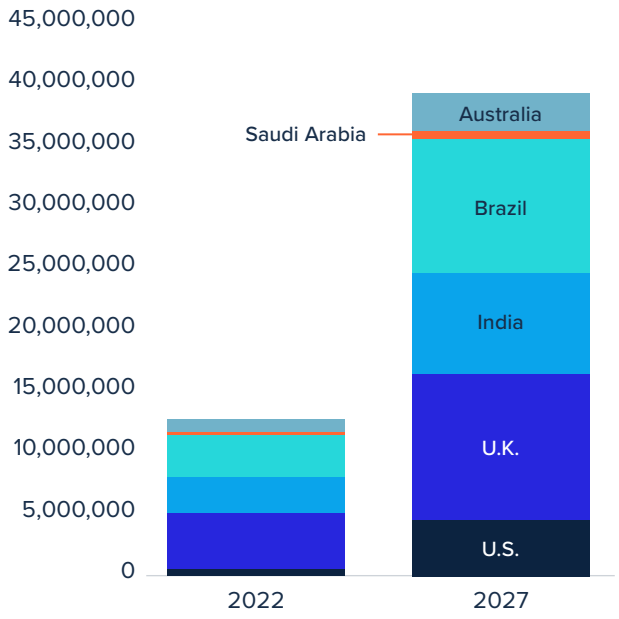

Brazil


Australia


Saudi Arabia

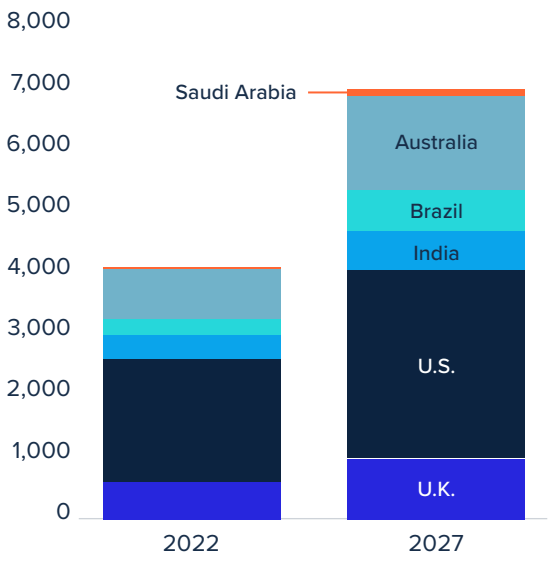

## Growth in Real-Time Payments (USD million)

**Combined 25 percent CAGR growth in Real-Time Payments**




## Growth in Scams (USD million)

**Combined 11 percent CAGR growth in APP scams**

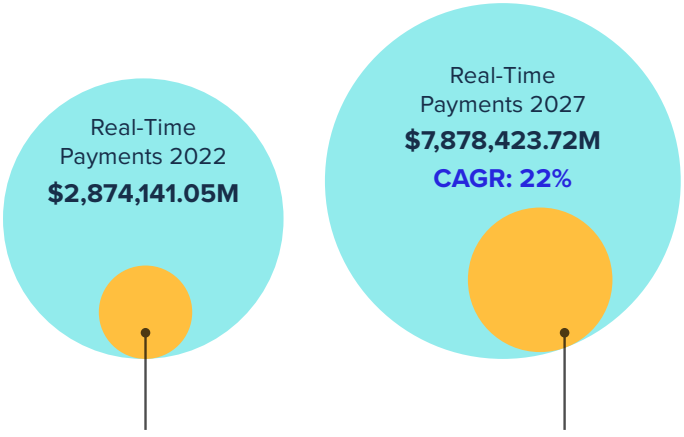


# Spotlight on **India**

The value of losses to APP scams in India is expected to increase by 9% between 2022 and 2027. While large, this is significantly lower than the forecasted growth in value of real-time payments, meaning banks can expect strong revenue growth without major increases in risk.

**Losses to APP Scams (USD), 2022-2027**


**Growth of APP Scams vs. Real-Time Payments (USD*), 2022-2027**




USD losses to APP scams
Estimated real-time payments value
**In million USD*

## How are consumers being scammed?

**41.6%**
I was asked to make a transfer to buy a product

**20.8%**
I was asked to make a transfer to invest in a product or company

**16.0%**
I was asked to make a transfer as an advance payment for a product or service

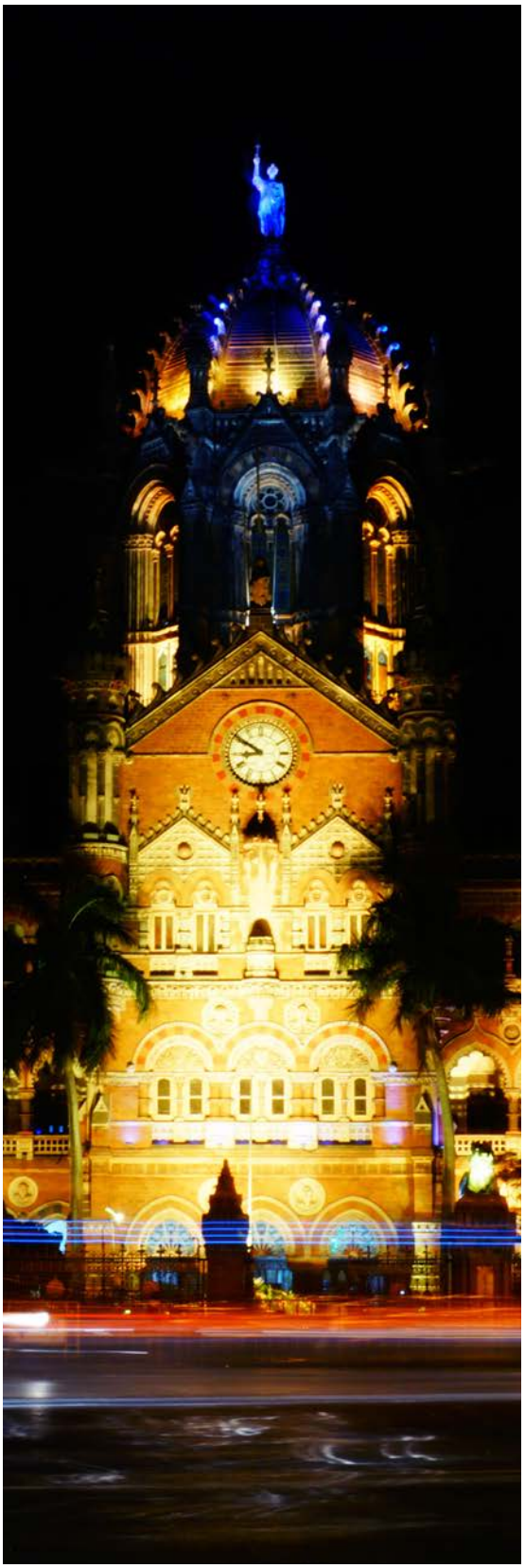
**8.8%**
I made a transfer to someone who pretended to be in a romantic relationship with me

**7.2%**
I was asked to make a transfer to pay an invoice or outstanding balance for a product or service

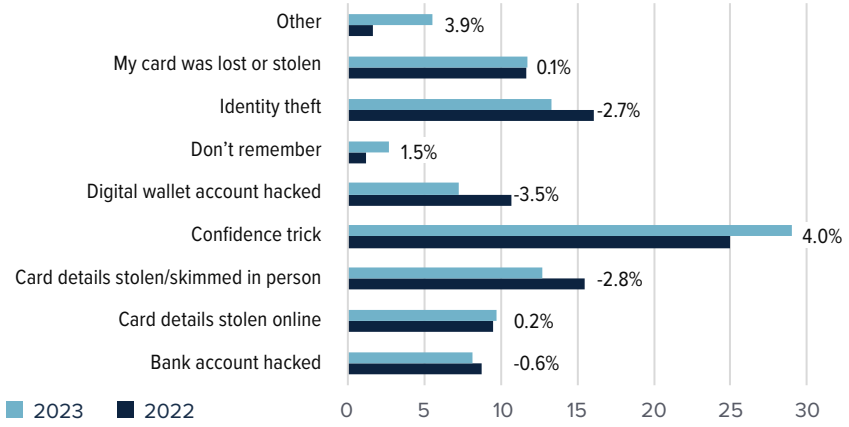
**2.4%**
I was asked to make a transfer by someone claiming to be a senior person in my company on behalf of the company

**1.6%**
I was asked to make a payment by someone claiming to be a trusted person or organization (such as the police or postal service)

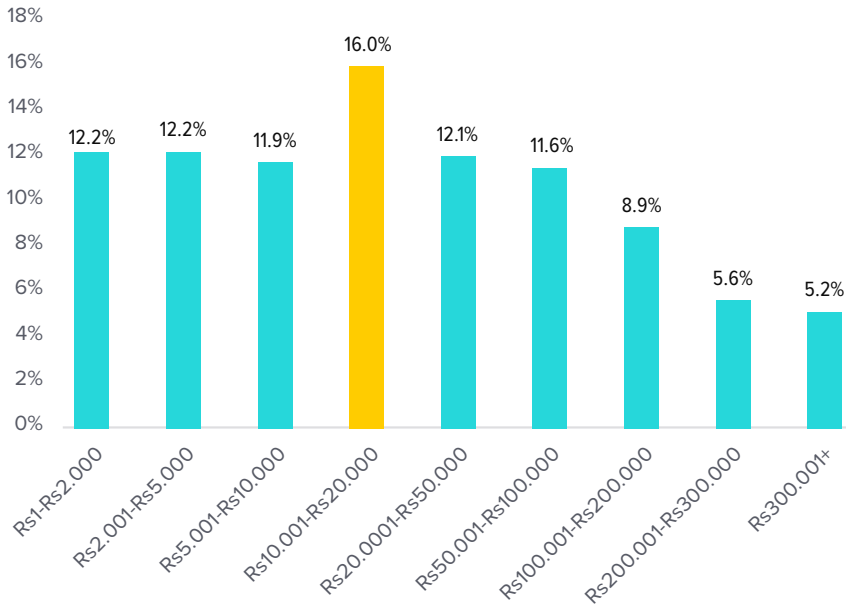
**1.6%**
None of the above



**Confidence scams remain a major risk to consumers, with fraudsters becoming ever more sophisticated and persistent.**




**Value of Fraudulent Transactions**




The ever-greater sophistication of scams seen in the market makes them difficult to spot for banks' rules-based anti-fraud systems. The job is made harder by the fact that most fraud involves losses on the low end, between 1INR and 1000INR, and so is more likely to be considered as routine activity. Machine learning solutions capable of detecting and adapting to anomalies in normal account behavior are more important than ever.

# Banks accelerating towards turning tables on scammers

In May 2023, transactions on India's Unified Payments Interface (UPI) hit a record 9 billion, illustrating the stunning extent to which payments in the country have shifted to digital platforms.[1] Aiding the transition is the penetration of digital devices: In 2023, there were 1.1 billion cellular mobile connections, equivalent to 77% of the total population.[2]

Unfortunately, this widespread digital take-up is not matched by widespread consumer understanding of the dangers posed by APP scams and other frauds. Despite the strong educational campaigns that accompanied the appearance of scams, fraudsters still find plenty of success using social engineering to develop targets from all demographics and all ages. Indian consumers are subjected to the full range of scams — romance, loan, account takeover and so on.

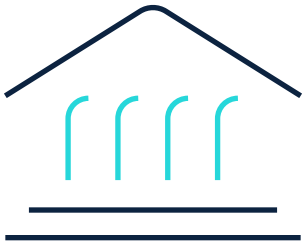
### Targeting by region — the "Jamtara" phenomenon

One peculiarity of the Indian scamming landscape is what can be called "targeting by region," whereby a specific location is subjected to concentrated attacks. The city of Jamtara in the state of Jharkand has become a byword for this. Over a period of months, it became a hub for organized cybercrime, spearheaded by a group of scammers posing as employees of banks and insurance companies. The scammers used social engineering to build relationships with victims, publishing cell phone numbers as customer service numbers for financial institutions. Today, once a network is broken by law enforcement, the scammers simply move elsewhere.[3]

### Banks fear loan scams most

Jamtara-style frauds have a relatively minor impact on banks' finances — it is loan scams that can cost them big. One common countermeasure is to set aside contingency funds from which to write off losses; another, in cases where misappropriated money has already left the receiving mule account, is to refund a percentage to the scammed customer.

These approaches are favored for several reasons. The first is relatively relaxed regulatory oversight: For example, the Reserve Bank of India (RBI) simply expects, or assumes, that financial institutions will protect customers' funds. How they do this is largely left to the institution itself. Second, where liability lies is unclear in India. Customers are usually regarded as liable the first time they are scammed, but thereafter, stronger security measures will come into effect — text messages asking the customer to confirm the authenticity of the transaction, for example. If these fail, banks tend to be held at least partially liable.



[1]Unified Payments Interface: https://en.wikipedia.org/wiki/Unified_Payments_Interface#:~:text=The%20Unified%20Payments%20Interface%20(UPI,%2Dmerchant%20(P2M)%20transactions.

[2]The state of digital in India in 2023: https://datareportal.com/reports/digital-2023-india#:~:text=The%20state%20of%20digital%20in%20India%20in%202023&text=India%20was%20home%20to%20467.0,percent%20of%20the%20total%20population.

[3]What is 'Jamtara' fraud: https://www.wionews.com/india-news/what-is-jamtara-fraud-in-indian-state-of-jharkhand-cybercrooks-con-2500-more-584265

**Banks are moving to become more proactive**

In the absence of firm regulatory mandates, and as scams become more sophisticated, forward thinking financial institutions are becoming more proactive on an individual level and also exploring ways to better work together at an industry level. These efforts would be greatly helped by technologies such as network intelligence, which facilitates the sharing of vital data signals between financial institutions, and by better leveraging AI and machine learning to monitor device and user behaviors, spot abnormalities and stop transactions in real time. Ultimately, the only way to be able to spot scams as they happen and to shutdown mule networks more efficiently is to improve data quality, the way that data is used and levels of collaboration.

Tools and approaches such as these will also help to brace financial institutions against emerging attacks, because once a new pattern is seen by one network participant, relevant information can be shared with the others. This level of knowledge is also readily available from technology partners, for example, who are well placed to fill this important consultancy role. Assets such as their libraries of AI- and statistical-based models enable banks to assess and attribute levels of risk to each transaction before deciding whether or not to permit it.

**A continuous learning curve**

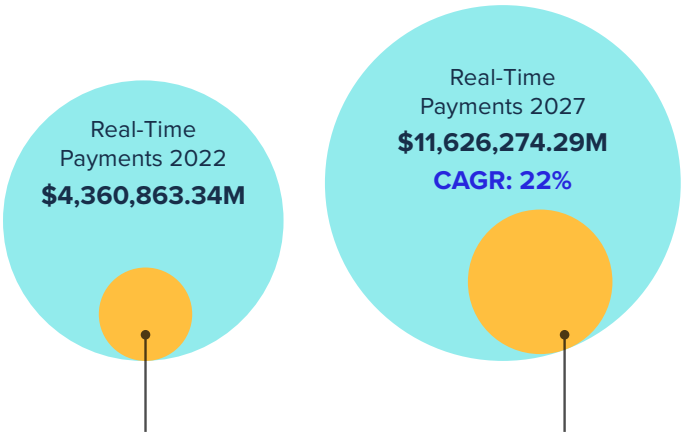
Indian financial institutions, like their counterparts elsewhere, are on a continuous learning curve when it comes to scam prevention. That curve was steep at the start, but is gradually flattening out as they become more adept at countering scams. Yet it will never decline. The way ahead is to continue exploring new, smarter technologies.

# Spotlight on the **U.K.**

The value of losses to APP scams in the U.K. is expected to increase with an annual compound rate of 10% between 2022 and 2027, but this is forecasted to be dwarfed by the growth in value of real-time payments — and therefore related revenue for banks — during the same period.

**Losses to APP Scams (USD), 2022-2027**


**Growth of APP Scams vs. Real-Time Payments (USD*), 2022-2027**




APP Scams Value 2022
**$587.17M**

APP Scams Value 2027
**$934.65M**
**CAGR: 10%**

USD losses to APP scams
Estimated real-time payments value
**In million USD*

## How are consumers being scammed?

**25.3%**
I was asked to make a transfer as an advance payment for a product or service

**24.1%**
I was asked to make a transfer to buy a product

**19.5%**
I was asked to make a transfer to invest in a product or company

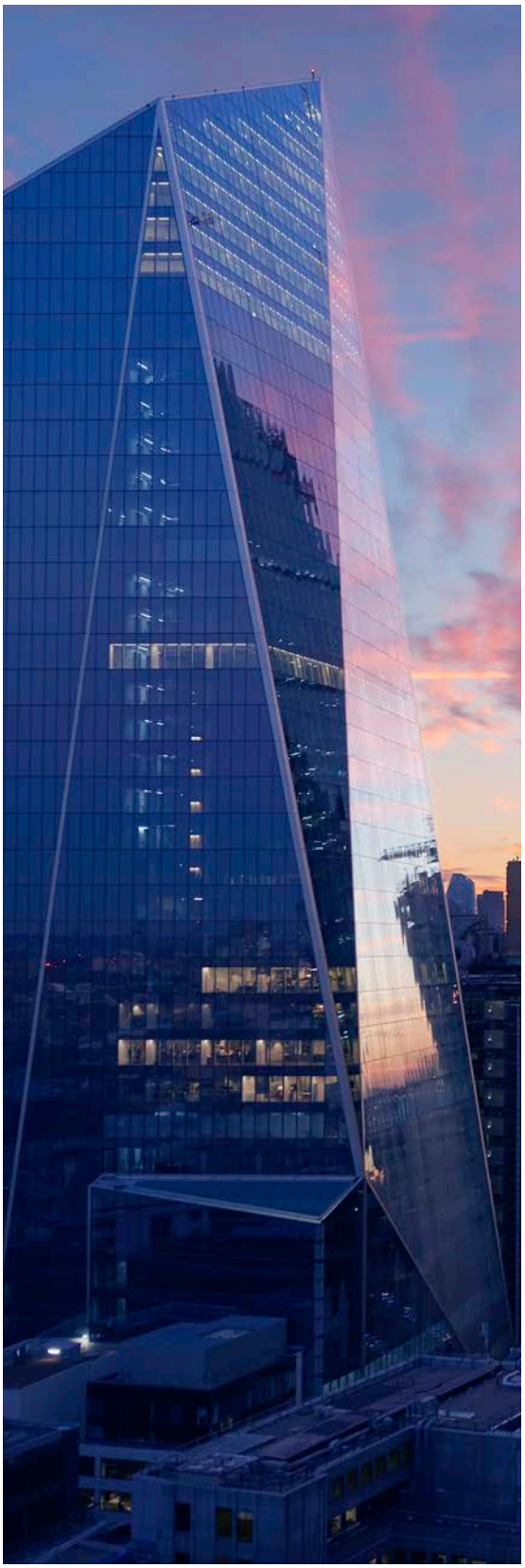
**9.2%**
I made a transfer to someone who pretended to be in a romantic relationship with me

**9.2%**
I was asked to make a payment by someone claiming to be a trusted person or organization (such as the police or postal service)

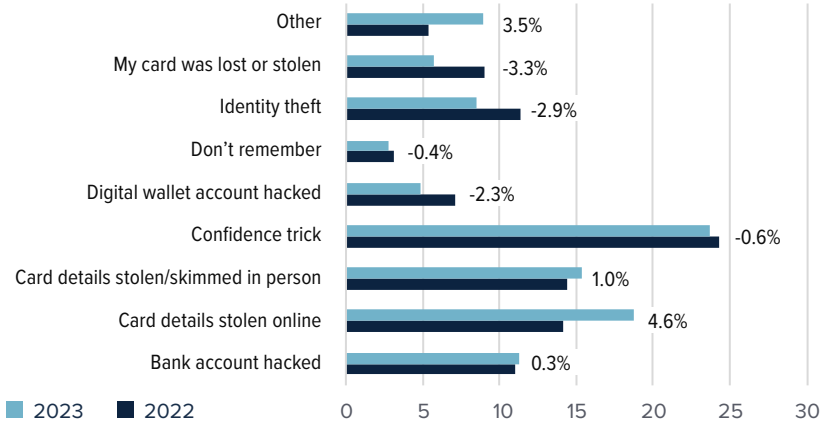
**5.8%**
None of the above

**4.6%**
I was asked to make a transfer to pay an invoice or outstanding balance for a product or service

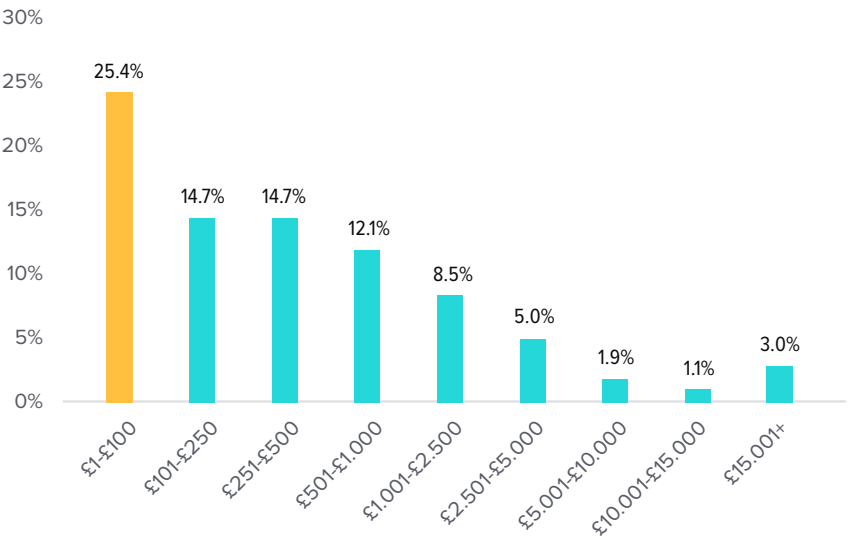
**2.3%**
I was asked to make a transfer by someone claiming to be a senior person in my company on behalf of the company



**Confidence tricks/scams are still the most common type of fraud in the U.K.**




**Value of Fraudulent Transactions**




A quarter of scams in 2023 involved amounts valued at £100 or less, and 54% involved amounts of £500 or less. Working within these limits allows fraudsters to hide their activity among the many hundreds of thousands or millions of genuine, routine purchases and transactions of similar value taking place at any given moment. The scale and velocity of these smaller ticket sizes illustrates why AI and robotic process automation (RPA) solutions are essential tools for monitoring and decision making.

# Landmark scams legislation brings clarity on key issues

The U.K.'s landmark Financial Services and Markets Act came into force in summer 2023, bringing banks, payment service providers (PSPs) and their customers some welcome clarity on key issues related to APP fraud, which caused gross losses of £249 million in the first half of 20224. The Act mandates 400-plus banks and PSPs to reimburse scammed customers, except in exceptional circumstances, for example. In addition, every six months the 12 biggest players must provide data demonstrating how they are reducing fraud.

The legislation is coming into force at a time when a steep rise in U.K. inflation has greatly increased the basic costs of living, providing fertile ground for mule account recruiters to flourish. In hard times, usually law-abiding account holders may be tempted to listen to a recruiter's proposal to make some easy cash. There is also a very real possibility that mandated reimbursement will encourage first-party fraud, whereby the payee suspects an item, offer or investment opportunity is too good to be true, but feels sufficiently protected to take the risk anyway.

**Collaboration is essential**

These new business conditions make it even more important for all players to share more information and do so in real time. A key driver is financial. Unlike other fraud types, where merchant chargebacks mitigate some reimbursement costs, APP frauds could prove very expensive for banks and PSPs, thus creating a big incentive to identify and close down the mule accounts that are the principal vehicle for fraudsters. Detection calls for 360-degree oversight of account activity, monitoring money in, as well as money out. Institutions already have systems in place to watch both sides of a transaction in the form of AML and fraud detection; countering APP scams calls for a new mindset that lives within a single solution.

**Greater care needed**

A further incentive for collaboration kicks in once mule activity is suspected or identified. Banks and PSPs should have the ability to proceed with greater care than previously practiced. The assumption pre-legislation was that identified mule accounts were typically assumed to be participants in the scam or at least complicit. With the ever-increasing emphasis on the need to both identify and close mule accounts, PSPs must tread cautiously before automatically flagging an account as a mule without strong evidence, as this risks wrongly accusing an innocent customer who may be the victim of violence or coercion at the hands of scammers in their search for "clean" accounts. While a PSP's first instinct might be to claim the gross negligence by the payee that absolves the organization of responsibility, the post-legislation environment creates the need for more caution.

The "debanking" furor in the U.K. in summer 2023 provided an illustration of the risks of arbitrary account closures. Intense media scrutiny revealed that some banks were refusing to open or maintain accounts for certain customers due to their political opinions. It is easier for the bank or PSP to justify reporting or closing a suspected mule account if it can show it has assembled evidence through working with the initiating bank or PSP.

[4]https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/new-app-fraud-legislation-is-coming/

### Spreading responsibility

The collaboration — and liability — issue gives rise to two questions. The first is, who is party to a scam? More and more, the financial institutions, who are only really at one end of the scam lifecycle, are beginning to feel that for too long they have been an easy target for regulators to place full financial penalty and that the ISPs, social media platforms and telcos must also be involved in discussions around solutions and liability. These players perform important roles in APP scams but currently take no financial responsibility. Financial institutions need to look out for technology that enables them to leverage network intelligence, making the whole ecosystem stronger.

The second question is, how might collaboration between PSPs work? The anti-scam measures described above are tailormade for AI: A typical AI scenario would be detecting the changes in behavior by a longstanding "clean" customer that are generally a sign of the account's new mule status. Between them, financial institutions, ISPs, telcos and social media platforms have access to enough data to make things significantly harder for scammers. Data points can be shared as signals between key players in restricted-membership groups via central processors — central banks, for example.

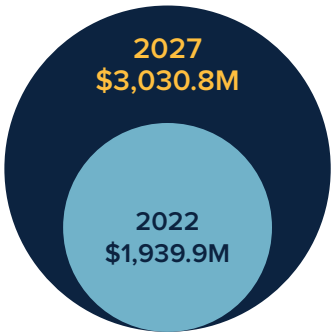
### Widespread public support

Surveys of public opinion about anti-scam measures suggest customers appreciate that banks and PSPs have a tough job to do and believe they are doing their best. Pushback against safeguarding features, such as Confirmation of Payee, is minimal. Maintaining this support as scam losses grow, however, will require greater collaboration and information sharing by players both inside and outside of the financial services industry.

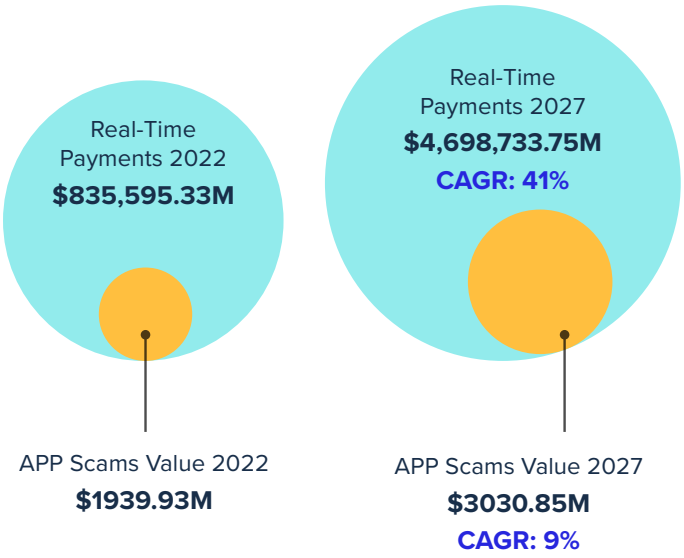
# Spotlight on the **U.S.**

The value of losses to APP scams in the U.S. is expected to increase by 9% between 2022 and 2027. But the growth in value of real-time payments is forecasted to far eclipse this as the bedding-in of the new FedNow® service within the wider payments landscape drives breakthrough adoption.

**Losses to APP Scams (USD), 2022-2027**




**Growth of APP Scams vs. Real-Time Payments (USD*), 2022-2027**




USD losses to APP scams
Estimated real-time payments value
**In million USD*

## How are consumers being scammed?

**23%**
I was asked to make a transfer to buy a product

**23%**
I was asked to make a transfer to invest in a product or company

**17%**
I was asked to make a transfer as an advance payment for a product or service

**10%**
I made a transfer to someone who pretended to be in a romantic relationship with me

**8%**
I was asked to make a transfer by someone claiming to be a senior person in my company on behalf of the company

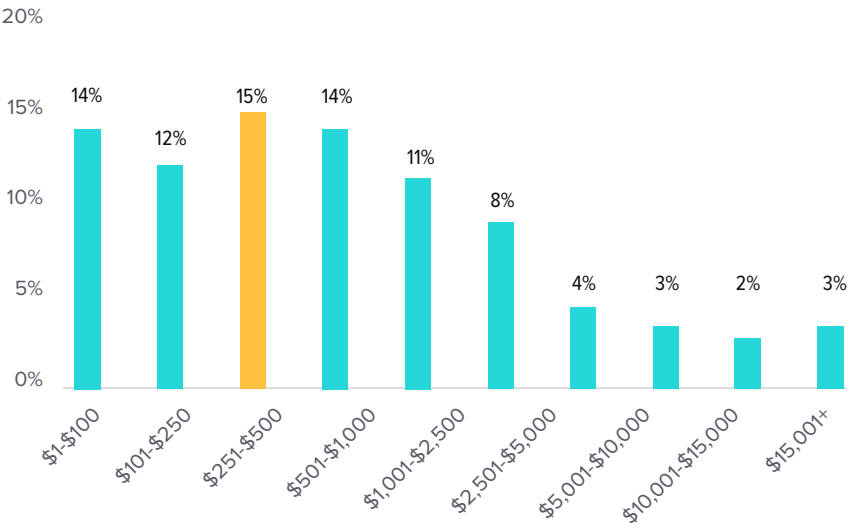
**7%**
I was asked to make a payment by someone claiming to be a trusted person or organization (such as the police or postal service)

**7%**
None of the above

**5%**
I was asked to make a transfer to pay an invoice or outstanding balance for a product or service

**Confidence tricks/scams remain firmly in the top three most common fraud types facing U.S. consumers.**


**Value of Fraudulent Transactions**




Four in 10 scams in 2023 involved amounts valued at $500, and nearly six in 10 (56%) involved amounts of $1000 or less, giving fraudsters the greatest possible chances of disguising their activity as routine purchases and transactions. As in other markets, the scale and velocity of these smaller ticket sizes illustrates why AI and RPA solutions are essential tools for monitoring and decision making.

# The FedNow Service provides opportunity to level-up fraud prevention

Financial institutions in the U.S. have achieved laudable gains when it comes to containing APP fraud. They're also making strides in building up capabilities for efficiently and reliably identifying and closing down the mule accounts used to move the proceeds of scams.

One factor working against them is the fatalistic attitude of the majority of scam victims who, whatever the size of their loss, often regard themselves as somehow responsible and don't report the scam. Financial institutions would also benefit in the fight against mule accounts if they made the relatively simple change of monitoring inward transactions rather than solely focusing outgoing funds.

**The FedNow Service changes the game**

The July 2023 launch of the FedNow Service is an opportunity for the payments community to make exactly these kinds of changes, and more. The FedNow Service has been developed by the Federal Reserve central bank to "facilitate nationwide reach of real-time payments services by financial institutions — regardless of size or geographic location — around the clock, every day of the year." With such an increase in scope for real-time payments, the time is right to take a proactive approach to fraud prevention.

This should involve strategies for tackling mule accounts, which start by looking beyond just the money leaving accounts and taking a holistic 360-degree view of inward and outward transactions. The volume of transactions is likely to grow (and it could explode), but that doesn't mean fraud protection teams will automatically get more resources or people, and so they need to work smarter.

Progress will be incremental, but institutions should prioritize having in place some form of AI or machine learning to support traditional behavioral profiling. Additional prevention measures already implemented by most institutions include text alerts checking the validity of transactions involving new payees.

As in other markets, collaborative, network intelligence-style information sharing between financial institutions will also be an important weapon against APP scams and other frauds. However, it is unlikely that calls to incorporate those other, unintentional enablers of fraud — telcos and social media — into the conversation around scam prevention and liability will make much progress.

**Plug the gaps to gain fast-mover advantage**

With the FedNow Service having placed PSPs' readiness for scam prevention firmly in the spotlight, PSPs will benefit from acting fast to plug gaps in their protection. For some time, scams have been under scrutiny at a congressional level, notably from Senators Elizabeth Warren and Robert Menendez. From their seats on the Senate Banking, Housing and Urban Affairs Committee, Warren and Menendez have conducted high-profile interrogations of the fraud prevention records of certain platforms, in particular the Zelle digital payments network.[5] The unwelcomed publicity for Zelle serves to illustrate the importance of fraud protection strategies when it comes to building trust and mitigating reputational risk, as other financial institutions join consumers in leaving the network.[6]

A recent article estimates losses of around USD 400 million owing to APP scams coming from Zelle, accounting for 21% of overall APP scam fraud losses in the USA.[7] This raises concerns about whether the Consumer Financial Protection Bureau (CFPB) current pressure on Zelle, along with the pressure from Congress in faster payments, are sufficient to reverse these trends in APP scams. For financial institutions, this means they will need to continue to expand their fraud strategies with further fraud intelligence and AI on both incoming and outgoing faster payments to adapt to this rapidly changing payments' landscape to stop scams and mule accounts.

As real-time transactions for the U.S. accelerate, scams tend to follow, hiding behind the rails of faster, instantly settled payments. Scammers, or bad actors, are on the lookout for opportunities to capitalize. For the financial institutions, a lot more is at stake — their brand reputation, consumer trust and ability to generate revenue and grow market share. The better their platforms are at detecting suspicious activities and making sure that their account holders are protected, the better their chance is to evolve and establish their brand identity.

[5]Sen. Warren says big banks fail to prevent 'rampant fraud' on payment platform Zelle: https://www.cnbc.com/2022/10/27/sen-elizabeth-warren-requests-cfpb-investigation-into-zelle.html

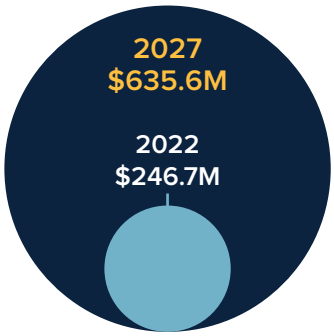
[6]https://www.wsj.com/articles/small-banks-warn-they-might-have-to-drop-zelle-over-scam-payment-costs-11670849934

[7]https://www.biocatch.com/blog/zelle-impersonation-scam-reimbursement

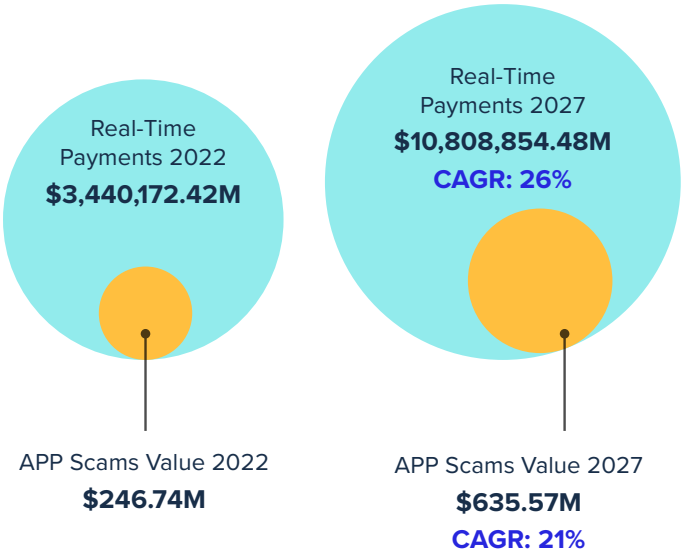
# Spotlight on **Brazil**

The value of losses to APP scams in Brazil is expected to increase by a CAGR of 21% between 2022 and 2027. But with the growth in value of real-time payments expected to be higher, banks can expect revenue and profitability to also increase at a faster rate, mitigating the financial impact of scams in the medium term, at least.

**Losses to APP Scams (USD), 2022-2027**




**Growth of APP Scams vs. Real-Time Payments (USD*), 2022-2027**




USD losses to APP scams
Estimated real-time payments value
**In million USD*

## How are consumers being scammed?

**27.0%**
I was asked to make a transfer as an advance payment for a product or service

**20.0%**
I was asked to make a transfer to buy a product

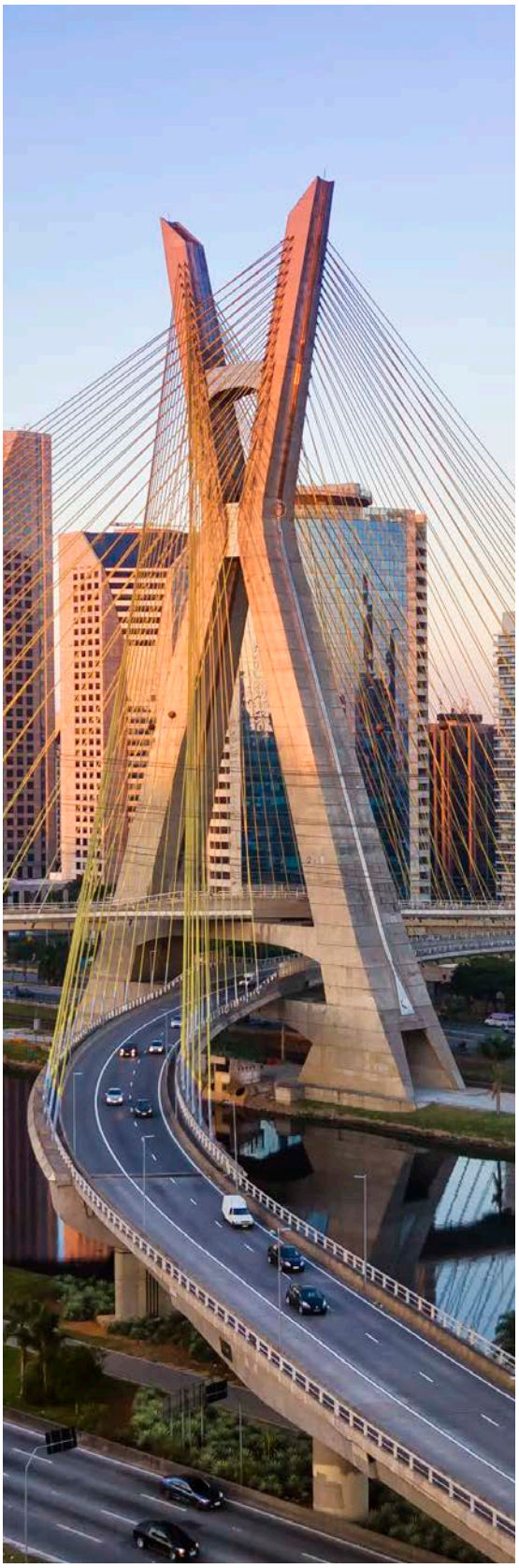
**17.0%**
I was asked to make a transfer to invest in a product or company

**13.0%**
None of the above

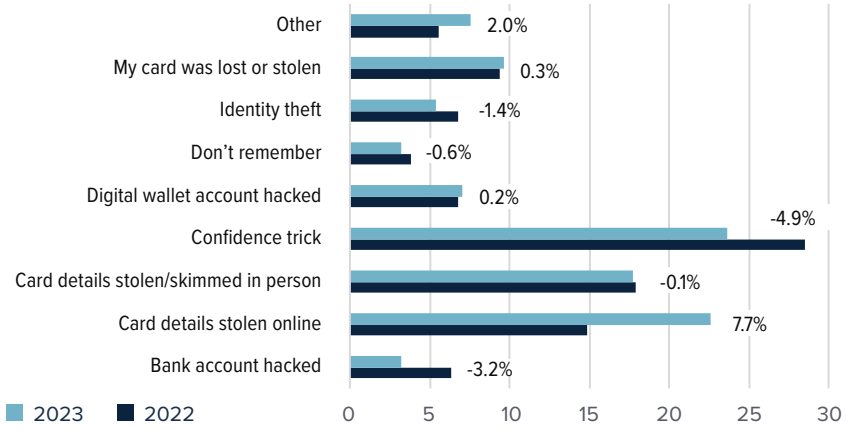
**10.0%**
I was asked to make a transfer to pay an invoice or outstanding balance for a product or service

**7.0%**
I made a transfer to someone who pretended to be in a romantic relationship with me

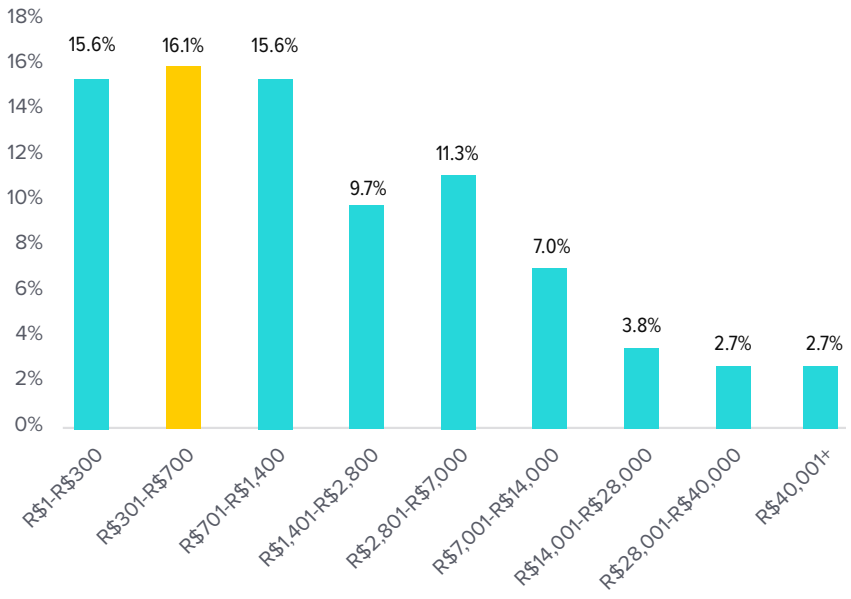
**7.0%**
I was asked to make a payment by someone claiming to be a trusted person or organization (such as the police or postal service)



**Slight decline in confidence tricks not enough to knock scams from the top spot when it comes to fraud risks facing consumers.**




**Value of Fraudulent Transactions**




More than 60% of fraud in Brazil in 2023 involved losses in the low to average range. As in other markets, this value bracket is a key target for fraudsters looking to hide their activity among the huge volume and high velocity of genuine transactions at this level. This kind of fraud will continue to be a problem for Brazil's banks without sophisticated, responsive machine learning solutions.

# Decentralization drives financial inclusion — but opens doors for scams

The enthusiasm with which the Brazilian population has adopted the PIX real-time payments platform, and the subsequent boost to financial inclusion, has been extremely welcome. But it has also created fertile ground for APP scammers.

The Central Bank of Brazil (BCB) introduced PIX in November 2020 as a more inclusive, democratized and decentralized alternative to the TED EFT system. It has certainly increased inclusion, introducing millions of previously unbanked Brazilians to digital payments. The latest figures show PIX has over 130 million individual users (almost two-thirds of the population) and accounts for more than 30% of all transactions in 2022.[8]

More than 700 financial institutions participate in PIX. The pertinent point, as far as scams are concerned, is that this figure includes many smaller players to whom the BCB has granted "payment initiator licenses," authorizing these organizations to initiate and receive PIX payments and transfers for their customers.

### Scammers are riding the slipstream of PIX's success

It is here that the downside of PIX's success can be seen, because these smaller players' KYC processes and tools needed to detect fraudulent transactions are not keeping pace with the rate at which they are gaining new accounts. This makes identifying the mule accounts that allow scammers to spirit away stolen funds difficult, since detection depends on monitoring both inflows and outflows of money. Larger institutions are more likely to have the systems in place to do this — though they may not always use them — but PIX's decentralization allows for these players to be bypassed, and with them, a strong layer of control that is otherwise present for more traditional payment types.

Exploiting or manipulating others to open or handover access to PIX accounts held with smaller, less well-protected financial institutions makes it increasingly easy for scammers to convert their schemes to cash. They no longer have to resort to such crude tactics as dragging a kidnapped account holder from ATM to ATM, though kidnapping remains a popular way to force people to authorize PIX payments to mule accounts.

### SaaS democratizes access to state-of-the-art scam detection tech

Fortunately, payment solution providers are democratizing state-of-the-art security systems by bringing to market SaaS solutions that enable smaller players to match the fraud detection capabilities of the bigger institutions. For example, network intelligence — the sharing of vital information in the form of anonymized data signals — facilitates collaboration between all parties to a transaction and leaves scammers with far fewer places to hide. Further measures include technology for determining the location of potentially fraudulent activity using mobile signal triangulation. Machine learning and AI can even be used for emotion and voice analysis to detect whether a payment initiator might be acting under duress.

The kind of network intelligence described aligns with new regulatory requirements that came into force in November 2023. BCB Resolution No. 6 requires financial institutions to share with each other data and information around payments fraud (whether successful or attempted) within 24 hours of detection.

The scope of required data would appear to cover suspected or confirmed mule account activity. Examples include occurrences or attempts of fraud related to opening or maintaining a deposit account or payment account and monitoring across the entire payments ecosystem, including PIX transactions and withdrawals.

[8]https://www.fintechnexus.com/in-two-years-pix-became-the-most-used-means-of-payment-in-brazil

**Can "super apps" supercharge scam prevention?**

As a relative newcomer to real-time payments, but one that has achieved massive scale in a short space of time, Brazil has both advantages and disadvantages in scam prevention. On the one hand, it is discovering the challenges that come with the rapid adoption of real-time payments. On the other hand, it has the opportunity to benefit from the anti-fraud technology developed in other regions. One area in which the country is innovating is that of PIX-enabled "super apps," which are a positive result of the banking decentralization.

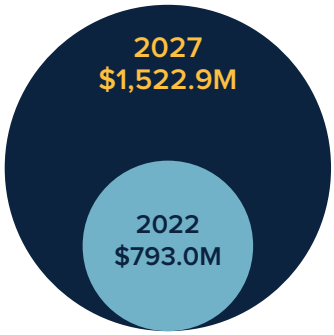
Mercado Livre, for example, is one such a super app: Within the one ecosystem users can buy or hire products, pay for subscriptions and conduct a host of other transactions. For Mercado Livre, the benefits are considerable: By holding the PIX accounts of both buyer and seller, the money never leaves the ecosystem; this is also a major disincentive for scammers. This enables Mercado Livre to reduce the costs to both parties, delivering greater value and security than consumers are currently getting from the wider ecosystem made up of multiple players. This approach gives the best of two worlds: security on a par with keeping real-time payments in the hands of the banks, but without constraining the user experience.

# Spotlight on **Australia**

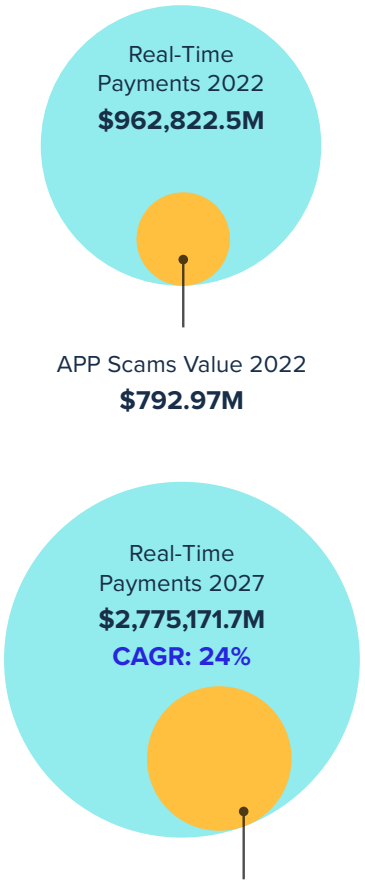
Scams are pressuring issues, increasing in volume and causing significant impact for both financial institutions and their customers. Banks play a critical role in the payments ecosystem, as do other parties, including schemes, regulators, technology and telecommunication providers.

The value of losses to APP scams in Australia is expected to increase at a compound annual growth rate (CAGR) of 14% between 2022 and 2027, while the value of real-time payments is expected to increase at a CAGR of 24% during the same period. This means revenue for banks from real-time payments is expected to grow faster than the risk of loss.

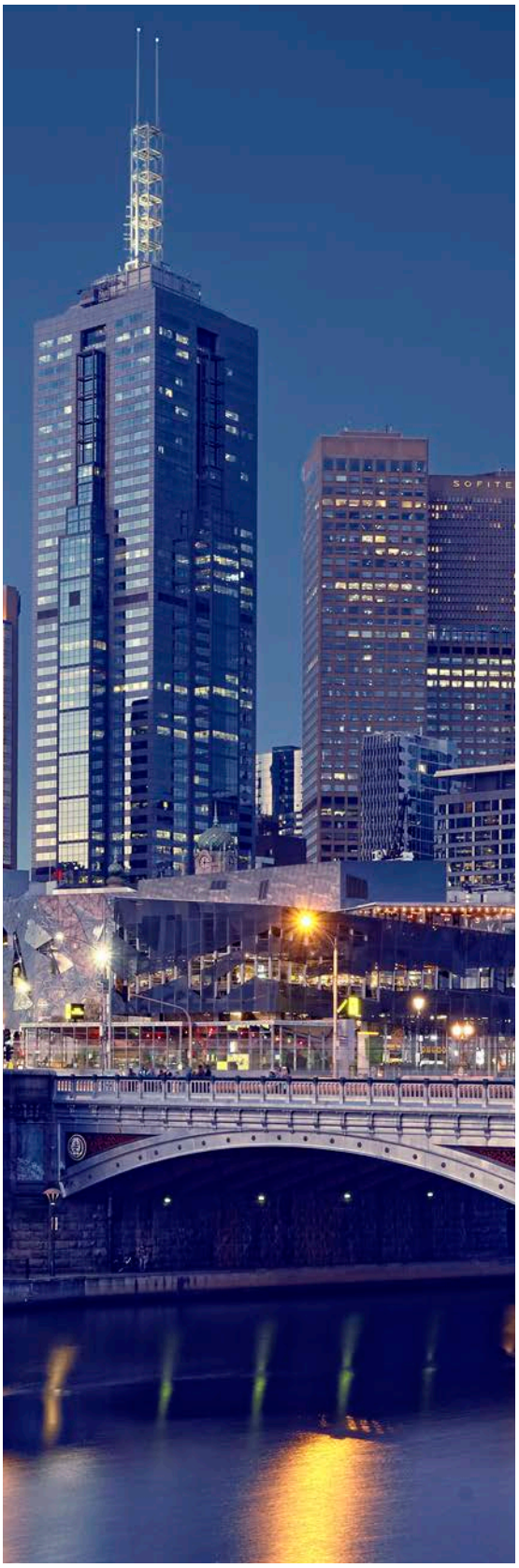
**Losses to APP Scams (USD), 2022-2027**



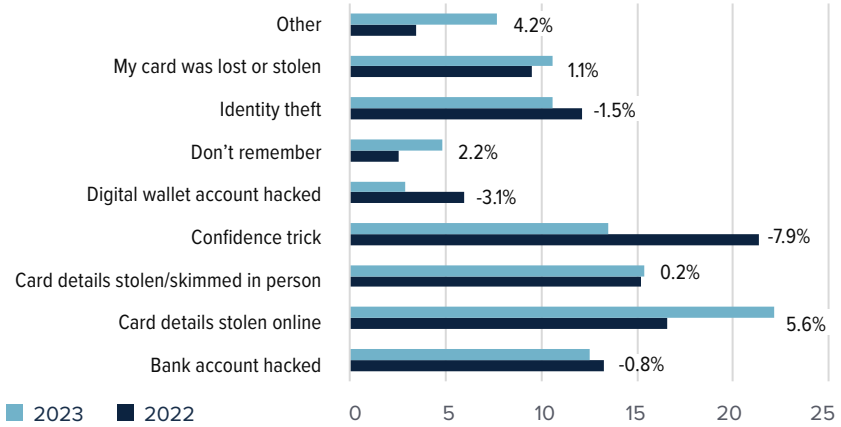

**Growth of APP Scams vs. Real-Time Payments (USD*), 2022-2027**



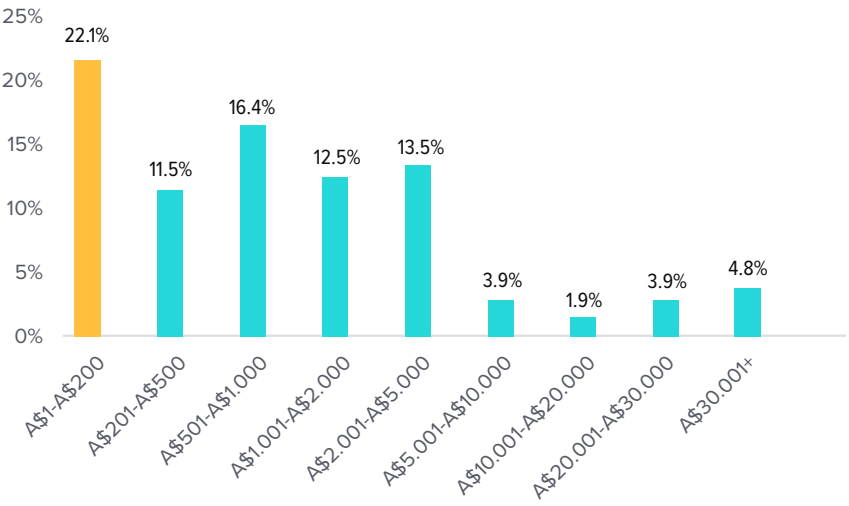

USD losses to APP scams
Estimated real-time payments value
**In million USD*



**The good news is that confidence tricks (which include APP scams) are in decline, indicating increased awareness among consumers and pointing to a win for industry-wide education campaigns.**




**Value of Fraudulent Transactions**




Half of APP scams in Australia in 2023 involved losses in the range of A$1-A$1,000. Fraudsters assume, often correctly, that transactions at this level are easier to hide from banks' rules-based detection systems, since they fit the pattern of routine purchases and transactions. Banks require sophisticated machine learning solutions that outperform rules-based engines to catch and prevent these scams.

## A lot to play for, and lots of players

Renowned early adopters of technology, Australian consumers are typically quick to take up new payment innovations. And as fast as new methods have appeared, scammers — also keen early adopters — have exploited people's willingness to trust in order to get around tech-based anti-fraud safeguards and perpetrate APP scams. Common scams include fraudsters masking their phone details to persuade a bank's customers that their calls and SMS messages are genuine, or intercepting emailed invoices and changing payment details to divert payments into and through the networks of mule accounts, without which APP schemes would be harder to get away with.

### The big question

Australians are accustomed to refunds on fraudulent credit card transactions, as reflected in our data. But new payment platforms and new scams have given rise to intense debate about where the burden of compensation falls. A close eye is being kept on the impact on banks of new legislation passed in the U.K., which compensates scammed customers in almost all instances and generally splits liability evenly between sending and receiving banks. A number of Australian consumer groups are advocating that the government adopt similar measures. However, the major Australian financial institutions are pushing back, arguing that such a soft touch will make customers less vigilant and scammers more active. Instead, they argue, customers themselves have a role to play in their own protection, and the protection and liability burden should be shared with other players whose platforms scammers also make use of.

### Should social media and telcos take some responsibility?

In particular, there are growing arguments for social media platforms and telcos to acknowledge degrees of responsibility for enabling scams to take place. Most scams originate on social media and messaging platforms, and the 80% of the population now on social media platforms represent a bigger, all-age target for scammers than was the case when older, less tech-savvy users were the most likely victims.[9] As for telcos, measures have been floated along the lines of those taken in the Philippines, where telcos are mandated to block messages containing links and disable the originating devices.

While the debate continues, banks have to find their own ways to prevent scams and to simultaneously deliver both frictionless transactions and effective protection to customers. Some suggest that one solution is to delay payments for up to 24 hours in cases where money is intended for a new payee or going to a new country. Confirmation of Payee — as seen in the U.K. — also figures prominently in the debate, but Australian banks are hesitating due to the investment needed. As consumer groups point out, however, cost has not stopped Commonwealth Bank introducing its NameCheck security check, which confirms payee details for first-time transactions.

[9]https://datareportal.com/reports/digital-2023-australia#:~:text=The%20state%20of%20digital%20in%20Australia%20in%202023&text=There%20were%2025.31%20million%20internet,percent%20of%20the%20total%20population

### Fraud? Scam? Or first-party theft?

One barrier to the fair distribution of liability is how different financial institutions distinguish between fraud — extracting funds from a customer's account without their knowledge — and a scam, where the customer is conned by the scammer into triggering a transaction or payment themselves, or revealing passwords. Definitions vary depending on institutions' internal policies, which in turn depend on, for example, the quantity and quality of the data points available. The issue is further complicated by a third component — first-party fraud, when a customer makes a payment or transaction fully intending to subsequently claim it is fraudulent.

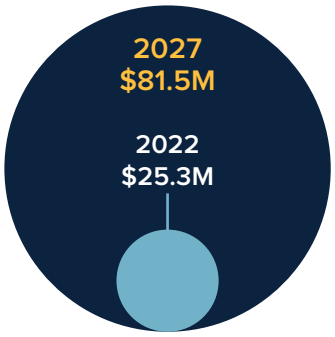
### The future is collaborative

Improving both data quality and levels of collaboration between financial institutions would be a more effective anti-scam model than that seen in the Australian market today. Better protecting customers from scams will only be possible if banks, telcos, social media platforms and, of course, payment software and solution providers, can facilitate the sharing of information from all sides of a transaction. Only with this kind of network-wide intelligence will it be possible to decide accurately and quickly if a payment is likely to be part of a scam or whether an account is being used as a mule.

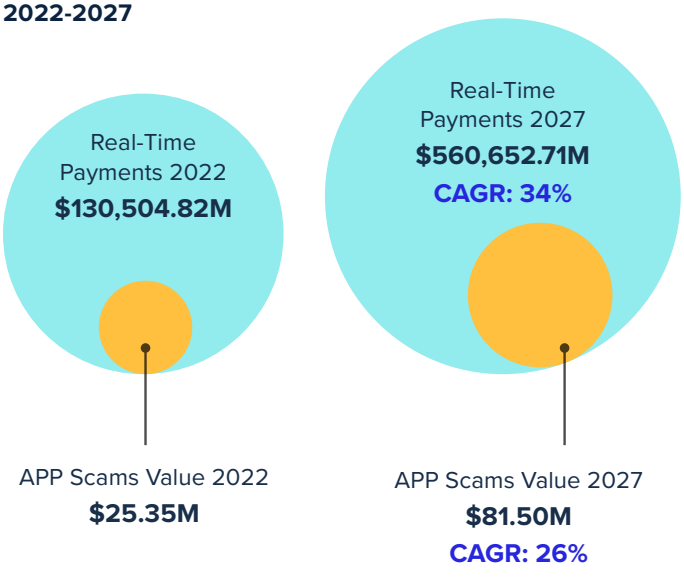
# Spotlight on **Saudi Arabia**

The value of losses to APP scams in Saudi Arabia is expected to increase by an annual compound rate of 26% between 2022 and 2027. This increase appears large, but it is from a low base and is less indicative of an emerging scams epidemic and more a sign of strong growth in digital payments overall. It is also significantly lower than the forecasted growth in value of real-time payments — and therefore related revenue for banks — during the same period.

**Losses to APP Scams (USD), 2022-2027**




**Growth of APP Scams vs. Real-Time Payments (USD*), 2022-2027**




*In million USD

## How are consumers being scammed?

**33.3%**
I was asked to make a transfer to buy a product

**15.9%**
I was asked to make a transfer to invest in a product or company

**14.3%**
I was asked to make a transfer as an advance payment for a product or service

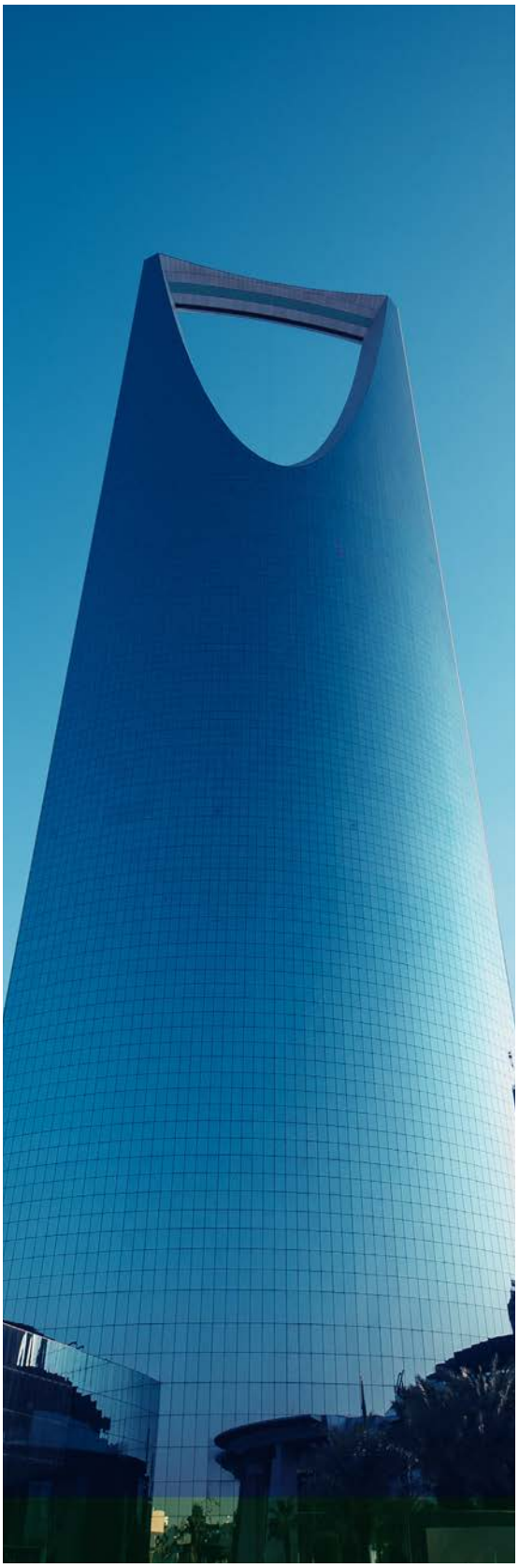
**12.7%**
I made a transfer to someone who pretended to be in a romantic relationship with me

**9.5%**
I was asked to make a transfer by someone claiming to be a senior person in my company on behalf of the company

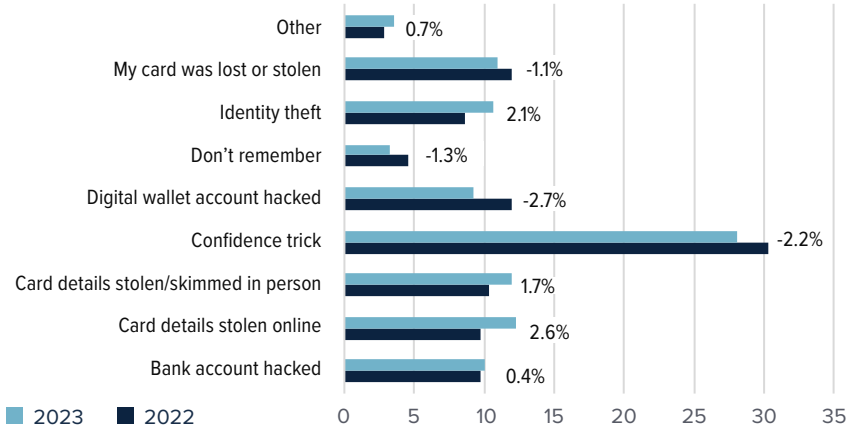
**6.4%**
I was asked to make a transfer to pay an invoice or outstanding balance for a product or service

**4.8%**
None of the above

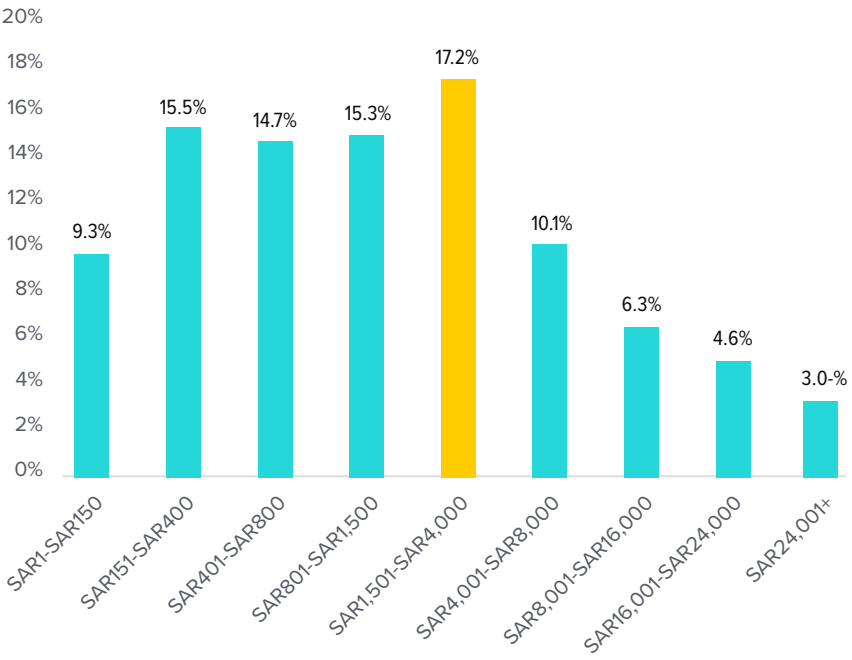
**3.2%**
I was asked to make a payment by someone claiming to be a trusted person or organization (such as the police or postal service)



**Confidence tricks/scams are way out in front when it comes to fraud experienced by consumers.**




**Value of Fraudulent Transactions**




In a pattern repeated throughout our study, the majority of scams in 2023 involved amounts at the lower end of the scale. This is a deliberate tactic used by fraudsters to bury their activity among the high volumes of genuine, routine purchases and transactions of similar value taking place at any given moment. The scale and velocity of these smaller ticket sizes illustrate why AI and RPA solutions are essential tools for monitoring and decision making.

# A market on an accelerated learning curve

Saudi Arabia, a relatively new real-time payments market, is already seeing the same variety of scams — investment, dating, romance, fake billing, remote access, identity theft — as seen in more established markets, targeting customers of all ages. Investment scams are particularly lucrative due to the country's relatively unregulated investment industry.

### Real-time fraud prevention is mandated

The most important feature of the regulatory environment when it comes to scams is a blanket requirement from SAMA, the Saudi central bank, which states that financial institutions must have in place real-time fraud prevention. It is up to banks to define what this looks like.

This reflects the fact that Saudi financial institutions are on a continuous (albeit accelerated, thanks to the government's ambitious modernization targets) scam prevention learning curve, just as they are for digital payments more generally — identifying, learning, responding and improving. The country started from a lower base because the launch of the real-time payment rails was not accompanied by a uniform distribution of fraud prevention controls.

### Investment on the up

Institutions are quickly gaining ground on the emerging breed of sophisticated scamming vehicles, such as "daisy-chained" mule accounts. Investment in fraud protection solutions is picking up, and payment solution providers report that the country's financial institutions — proven fast learners — have an increased appetite for consultancy-type support to learn about the prevailing trends in fraud worldwide. These positive signs for the future are largely due to the realization that uncontained scams weaken consumers' faith in financial instruments and ultimately threaten the modernizing potential of the market's payments innovation strategy.

### Get a head start on collaboration

As a market that is earlier on its real-time payments journey than the others in this report, and with a greater level of centralized regulatory control, Saudi Arabia is unencumbered by many of the obstacles to scam prevention seen elsewhere. This is a major advantage compared to other markets. For example, it has the opportunity to encourage or mandate banks to improve both data quality and levels of collaboration in order to be able to shut down mule networks more efficiently. Better protecting customers from scams will only be possible if banks can facilitate the sharing of vital information from both sides of a transaction. This kind of network-wide intelligence would make it possible to decide accurately and quickly if a payment is likely to be part of a scam, or whether an account is being used as a mule.

It may also be prudent for financial institutions and regulators in Saudi Arabia to monitor the debate taking place in other markets around which services and platforms are actually party to scams and could be held liable. Banks are only really at one end of scams; social media platforms and telcos perform important enabling roles, yet currently take no financial responsibility. Financial institutions, social media platforms and telcos must collaborate and share intelligence and signals to protect the consumer and create a scalable and secure environment.

ACI Worldwide Real-Time Payments | GlobalData.

# Afterword
## Act Now To Get Ahead of APP Scams

Real-time payment rails have the potential to be the most trusted and secure payment rails available. By refining the use of AI, embracing a higher level of payments intelligence and cracking down on mule accounts, the industry can leave the scammers with fewer places to hide and bring the growth in APP scams under control.

To get ahead on scams, banks are encouraged to strategize with these three key themes in mind:

1. **Accelerate the development of payments intelligence and seamless collaboration.** Mule accounts and behavioral anomalies indicative of scams can be more quickly identified when both payments in and out are being monitored and if you have 360-degree visibility of the behaviors of accounts on both sides of a transaction. This represents a new era of payments intelligence, one with smarter AI systems driven by stronger insights. And to bring it to realization, an industry-wide network and process for sharing anonymized fraud intelligence signals is needed.
2. **New regulations are imminent.** Scams are impacting a growing number of consumers, just as real-time payment rails are becoming increasingly important to national economies. That leaves regulators under pressure to resolve major questions around consumer compensation and institutional liability for APP scams, and many are keeping a close eye on the U.K. There, new rules mandate that institutions at the receiving and initiating ends of transactions share the costs of reimbursing ripped-off consumers. Banks should expect the lessons learned will influence regulatory responses elsewhere.
3. **To break the chain, focus on mule accounts — and incoming transactions.** The “business case” for scams depends on mule account networks, without which criminals would struggle to convert stolen funds to cash. Monitoring inward transactions rather than solely focusing on outgoing funds is a relatively simple change to make, but would represent a major leap forward in banks’ abilities to discover and disrupt mule account networks.

The technology already exists to help banks address each of these requirements and opportunities. For some time, we at ACI have discussed how network intelligence empowers all players involved in a transaction to exchange vital scam-busting signals, even leveraging the extended flexibility of ISO 20022, to transport machine learning metadata.

By working together and with their partners to take a more concerted and collaborative approach to leveraging these technologies, banks can finally turn the tide on scammers.



**LEARN MORE**
www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

**CONTACT ACI**
Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393



ATL1742 11-23