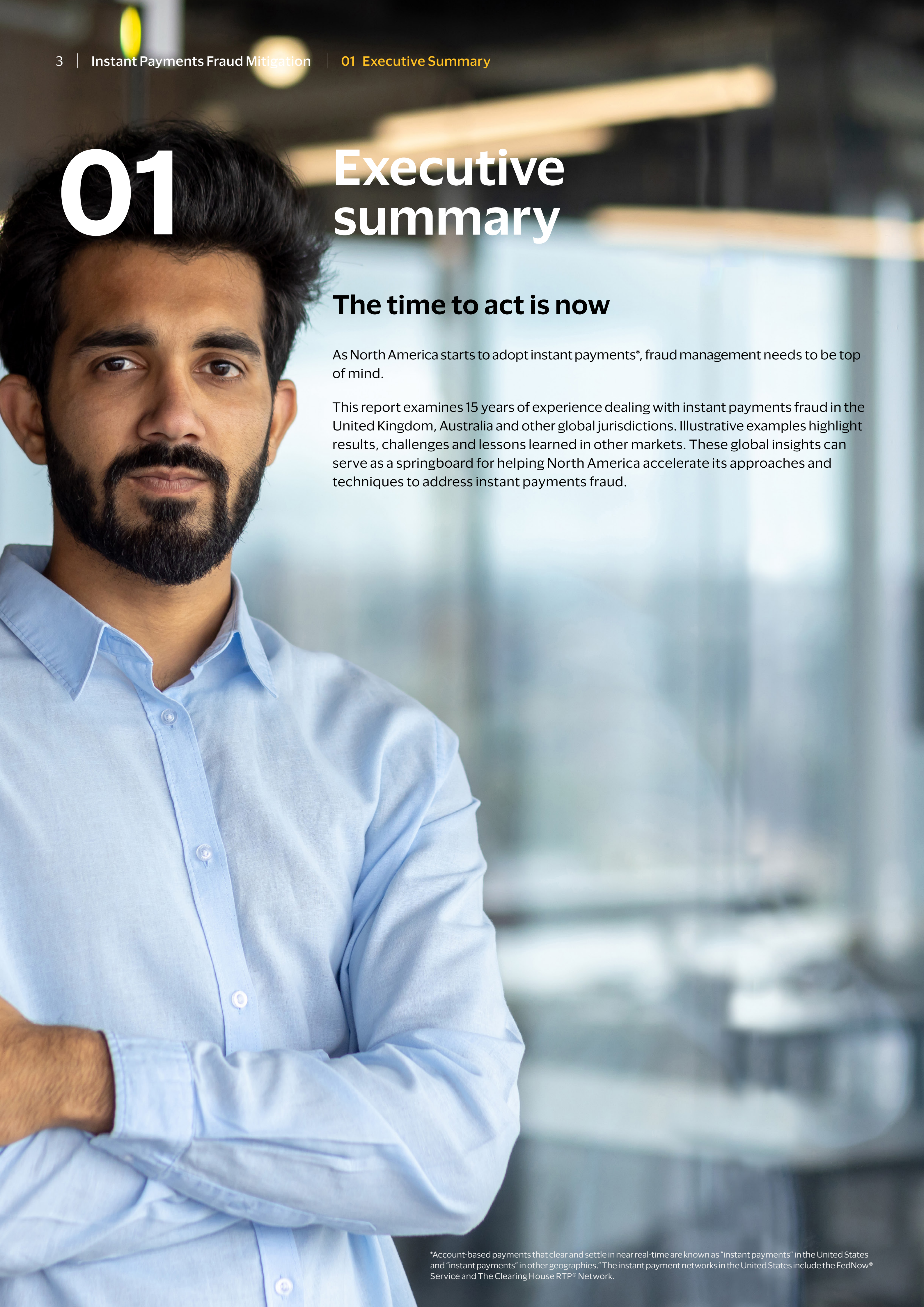
VISA | LIPIS ADVISORS

# North America Instant Payments Fraud Mitigation

## Applying global lessons learned

# Table of Contents



# 01 Executive summary

## The time to act is now

As North America starts to adopt instant payments*, fraud management needs to be top of mind.

This report examines 15 years of experience dealing with instant payments fraud in the United Kingdom, Australia and other global jurisdictions. Illustrative examples highlight results, challenges and lessons learned in other markets. These global insights can serve as a springboard for helping North America accelerate its approaches and techniques to address instant payments fraud.

*Account-based payments that clear and settle in near real-time are known as “instant payments” in the United States and “instant payments” in other geographies.” The instant payment networks in the United States include the FedNow® Service and The Clearing House RTP® Network.

# 1 | Instant payments have arrived

Instant payments are credit-push account-based payments. There are currently more than 60 instant payment networks either live or in development across the world.

The ability for a consumer or business to send an account-based payment 24/7/365 that is posted and available near-instantly with settlement finality has numerous benefits for industry stakeholders, such as reduced settlement risk for financial institutions and improved cash flow for recipients of instant payments. In addition, financial institutions, service providers, technology companies and others are investing in using the real-time rails to deliver new use cases and capabilities for their end users.

## North America instant payment networks

**Canada**

Payments Canada plans to launch a new instant payment network, called Real-Time Rail (RTR).

PAYMENTS CANADA

**United States**

There are two separate US instant payment networks. The Clearing House RTP® Network, launched in 2017, continues to see significant year-over-year growth from its 350+ participating financial institutions. The FedNow® Service was launched in 2023. Early adopters include 35 banks and credit unions, 16 service providers, and the U.S. Department of the Treasury's Bureau of the Fiscal Service. Both payment networks are expected to grow participants over time.

R | T | P® Powering Smarter Payments FedNow 24/7 INSTANT PAYMENTS

# 2 | Instant payments fraud increasing globally

Despite the benefits to end users, real-time money movement can create prime opportunities for financial crimes. Globally, instant payment networks have seen an increase in both authorized push payment (APP) fraud and unauthorized payment (UP) fraud.

Authorized push payment fraud in the United Kingdom (UK) rose by 40% between 2020 and 2021, resulting in losses of GBP 583 million (USD 706 million).[1] This was almost half of the total GBP 1.3 billion (USD 1.57 billion) lost to fraud. Furthermore, authorized push payment fraud exceeded card fraud in both 2021 and 2022.[2]

Other global markets have also seen sharp increases in instant payments fraud due to the growth in the volume and value of transactions, along with the emergence of social engineering to perpetrate authorized push payment scams, and sophisticated crime rings using mule accounts.

**Year over year APP increase in the UK**

**40%**

increase from 2020 to 2021

| | Authorized push payment (APP) fraud | Unauthorized payment (UP) fraud |
|---|---|---|
| **Definition** | When a sender is tricked into authorizing and sending a payment to the fraudster. | When a fraudster gains unauthorized access to a customer's credentials or has by-passed customer authentication to gain access to the sender's account. |
| **Means to perpetrate fraud** | The criminal impersonates a genuine individual or company and deceives victims. A range of methods such as email, text, phone, or social media can be used. | The criminal can use a range of tools, including phone numbers, malware, SIM cards, or information gained from data breaches. |
| **Examples** | Impersonation scam, romance scam, and advanced fee scam. | Identity theft (hacking, data breaches, etc.), SIM swap. |

# 3 | North America landscape vulnerable

The digital nature of instant payments allows fraudsters to operate without geographic boundaries. They frequently perpetrate crimes from any location and are well-versed in adapting successful techniques used elsewhere.

In other markets, it appears fraudsters adapt as the instant payment network ecosystem and use cases evolve. Fraud can be difficult to control once fraudsters have exploited gaps and mitigating solutions take time to implement.

The US market is uniquely vulnerable. Over time, up to 9,000 domestic financial institutions may join one or both networks with varying levels of risk identification and mitigation tools, which can slow the ability for the ecosystem to fully protect instant payments.

# 4 | Participants challenged to effectively address fraud

Fraudsters are agile and search for weaknesses in the payments value chain. At a minimum, instant payment solutions need to:

- Protect multiple points within the payments value chain including sending and receiving financial institutions, service providers, end users
- Employ techniques that provide a multi-pronged approach to thwart both authorized and unauthorized fraud
- Support a consistent fraud reporting framework to share and track developments transparently to stakeholders
- Acknowledge that fraudulent payments may start on one payment rail (e.g., instant payments) and then move to another payment rail (e.g., ATM cash out)

# 5 | Industry collaboration necessary to effectively address fraud

No individual stakeholder can single-handedly prevent instant payments fraud. Central infrastructures, payment networks, financial institutions, service providers, technology companies, and end users each have a role in detecting and mitigating financial crimes. Some solutions may require full participation and benefit from mandated scheme rules.

Collaboration within the payments community and beyond is needed to implement and evolve solutions to address financial crimes using three primary solutions:

## Technology

Technology solutions can help identify and prevent fraudulent transactions in real-time at both the central infrastructure and individual financial institution levels.

## Scheme rules

Mandates can help to ensure consistent usage of fraud identification and mitigation tools, as fraud mitigation is only as strong as the weakest link in the payments value chain.

## Awareness

“Smart friction” can help end users be aware of when they are at risk and get them to think twice before initiating a transaction. Combining smart friction with alerts can increase end-user confidence in their payment experience.

# 02 Landscape overview

## Instant payments present financial institutions & networks with new challenges on a 24/7/365 basis

## Instant payments fraud by the numbers

Fraud figures reflect an upward trend in the value of instant payment losses between 2020 and 2022, with some slowing between 2021 and 2022 in the UK.

Between 2020 and 2022, UK authorized push payment fraud value increased 15% from GBP 421 million to 485 million. After APP fraud value reached a high-water mark in 2021 of 583 million, it decreased 17% in 2022 to 485 million. The number of fraud cases increased 34% from 2020 to 2021, and continued to grow in 2022 although at a slower pace of 6%.[3]

Investment and romance schemes are the two predominate types of authorized push payment fraud in Australia. These scams increased in value 298% between 2020 to 2022 - from AUD 105 million to 417 million. Over this same two-year period, the average loss per victim for all reported fraud increased 150% to nearly 20,000.[4]

### United Kingdom

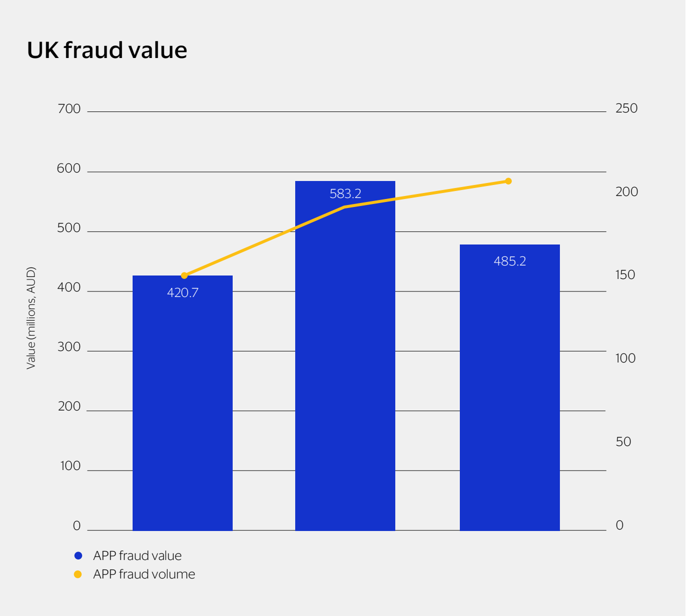
**15%**

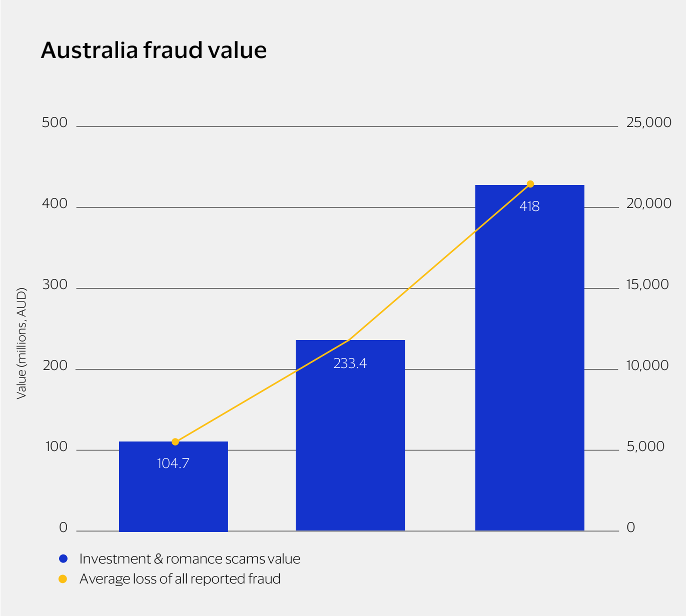
Increase in APP fraud value (2020 - 2022)

### Australia

**298%**

Increase in investment & romance scams value (2020 - 2022)


UK fraud value


Australia fraud value

# Participants face four major challenges to address instant payments fraud

## 1. Limited view

Financial institutions generally have inherently limited views across the entire payments value chain. The sending financial institution lacks insights about the receiver, and the receiving financial institution lacks insights about the sender, unless the sender and receiver are domiciled at the same entity.

While most sending financial institutions have employed fraud mitigation techniques when sending payments, there is little to no insight into the receivers. Instant payments allow senders to push money to receivers they may not know or are manipulated into making payments to fraudsters the sender believes to be legitimate (e.g., romance scams, investment scams). Frequently these authorized push payments are received by "money mules" who are individuals working as part of a scam to receive and quickly move money obtained from fraud victims. Some money mules are aware they have been recruited to help international crime networks steal money from victims; others may not realize they are facilitating fraud.

The lack of network-level insights limits the ability for both sending and receiving financial institutions to effectively mitigate fraud across the transaction lifecycle – from before the payment is sent, to the receiving financial institution's acceptance, and to aiding with recovery when fraud occurs.

## 2. Speed

Even if a financial institution has perfect information, it needs to ensure the sender is initiating a legitimate payments transaction in real-time. The receiving financial institution has milliseconds to either accept or decline the payment. Once accepted, the transaction instantly clears and settles, and the receiver has near instant access to the funds.

## 3. Inconsistent user experience

It's not uncommon for the end-user experience to differ throughout the payment lifecycle. For example, some apps may prompt the payee to confirm varying levels of payment details prior to the payment being made. And the process may differ for managing fraud victims between financial institutions, impacting the reimbursement policy and timing. All of this leads to confusion and a loss of trust in the financial system.

## 4. Gaps and lack of fraud reporting

Financial crimes can happen when there is a ripe opportunity to exploit weaknesses. Fraudsters may recognize weaknesses during times of change, such as when financial institutions are merging systems, or vendor platforms are being replaced.

Without a consistent fraud categorization framework across payment types and stakeholders, fraud insights can be limited. Furthermore, a patchwork of resources across the payments industry and law enforcement can create gaps for holistic reporting and remediation.

# 03 Global lessons learned and best practices

## North America can benefit from global experiences

This study focuses on instant payment lessons learned and best practices from other geographies to identify best practices that may be applied to stakeholders in North America. Solutions need to cover multiple points within the payments value chain to address emerging gaps.

The solutions are organized in three categories as described earlier that can address authorized push payment fraud and/or unauthorized fraud for sending and receiving participants:

- **Technology**
- **Scheme rules**
- **Awareness**

Various techniques can be used for these solutions as shown below. While this list is not exhaustive, it illustrates fraud mitigation approaches used in other markets to fill gaps.

| Mitigation solution | Techniques | Function | Type of fraud | |
|---|---|---|---|---|
| | | | APP | UP |
| **Technology** | Fraud monitoring system | Uses fraud-scoring at the central infrastructure level to provide insights to sending and receiving financial institutions. This needs to be combined with information-sharing to utilize network-level data | N/A | ✓ |
| | Biometric tools | Uses biometric tools (e.g. fingerprint, iris scan, facial recognition) to authenticate users prior to sending a payment | ✓ | ✓ |
| | Behavioral analysis | Uses data to categorize and analyze user-level behavior and identify anomalies in either payments information (i.e. sending payments to an unknown person or entity) or in the user's usage of the service (i.e. incorrect PIN input, abnormal location data, unusual time of initation) | ✓ | ✓ |
| | Confirmation-of-Payee (CoP) | Allows the sender to confirm the name related to the receiver's alias or account information prior to sending a payment | ✓ | N/A |
| | Digital identity | Uses a secure digital ID to verify a sender's identity | N/A | ✓ |
| **Scheme rules** | Limits and transaction holds | Provides flexibility to define limits and hold times such as:<br>- Transaction value limits: Value limits for individual transaction or during certain time windows<br>- Velocity limits: Daily, weekly, monthly limits on the number of payments sent or received<br>- Transaction holds for analysis: Rules that enable participants to conduct more detailed fraud analysis on transactions despite standard scheme SLA requirements | ✓ | ✓ |
| | Enhanced authentication measures | Uses an extra layer of security to authenticate the end user (e.g. SCA/MFA) | N/A | ✓ |
| | Dispute resolution/ loss recovery | Uses rules and/or regulations regarding fraud resolution/loss recovery for consumer protection purposes | ✓ | ✓ |
| **Awareness** | End user education | Facilitates user awareness about safety and precautions to protect against payment fraud (e.g. campaigns such as "Take Five to Stop Fraud") | ✓ | ✓ |
| | Fradulent individual database | Provides a database for sharing fraud-related data between multiple parties, especially on known fraudsters | ✓ | ✓ |
| | Cross-industry collaboration | Facilitates efforts for cross-industry collaboration to collectively address payment fraud mitigation (e.g. financial services, law enforcement, telcos) | ✓ | ✓ |

# Technology

## Fraud monitoring system

**Central and local fraud monitoring systems can help participants make better decisions.**

Fraud monitoring systems, especially those operated by the central infrastructure, are increasingly being used in global markets to:

- Provide fraud scoring services
- Track money movement
- Identify potential money mule accounts

Central infrastructures should have the visibility to raise red flags on suspicious transactions, track money movement when fraud does occur, and identify suspicious payment activity. However, these systems are best seen as supplements to financial institution-led efforts, not replacement systems. Instead, they should be designed to provide financial institutions with insights to make more informed payment risk decisions than would otherwise be possible.

### Key takeaways

- Central infrastructures are being increasingly tasked with identifying potentially fraudulent transactions
- Centralized monitoring can aid with providing fraud-scoring services, tracking money movement when fraud does occur, and identifying potential money mules

See fraud monitoring system country highlights from the UK and Brazil

## Biometric tools

**Biometric tools can add a layer of security; privacy and AI considerations may create challenges.**

Biometric tools use various technologies to authenticate a user prior to sending a payment using physical features such as fingerprint, iris scan, facial recognition, voice, etc. These tools are based on the user's physical features. Biometric identifiers are almost exclusively permanent. If an unauthorized party gains access to that data, it cannot be easily changed making it difficult for an individual to regain control and prevent misuse.

Voice biometrics, for instance, identify different sounds to recognize the unique characteristics of an individual's voice, such as tone, pitch, and rhythm, and use them to authenticate the user's identity. While biometric tools add a layer of security because the information has historically been considered hard to be stolen or compromised, there are privacy concerns that stem from the technology. Furthermore, advances in artificial intelligence (AI) mean that some tools, such as voice recognition, can be circumvented.

### Key takeaways

- Biometric tools utilize physical features that are unique to each user, but can raise concerns regarding data privacy and security of personal information
- The rise of AI and machine learning (ML) to create so-called "deep fakes" make voice detection less dependable. While facial recognition and fingerprint technology are not fool-proof, they are currently much harder to fake and require physical proximity to the potential fraud victim, making them stronger than voice recognition in the age of generative AI

See biometric tool country highlights from the UK, the Netherlands Australia and Brazil

# Technology

## Behavioral analysis

**Behavioral analysis has promise in identifying abnormalities.**

Behavioral analysis tracks how end users use their devices and notifies them of suspicious behavior using phone calls, email, or other modes of communication, such as in-app notifications.

Behavioral analysis is well suited to address unauthorized payment fraud due to the specificity of how one uses their device, which can be extremely difficult for fraudsters to replicate. This can also help against authorized push payment fraud if the transaction is atypical enough to trigger warnings, though this is by no means a silver bullet.

Environment detection, a subset of behavioral analysis, identifies the environment in which the caller is located, detecting background noise, echoes, etc. This can help with account takeover fraud by sending alerts when a payment is being initiated from a location that does not correspond with the user's known location.

The effectiveness of behavioral analyses may weaken over time with the increased capabilities of AI/ML.

### Key takeaways

- Behavioral analysis offers substantial promise to help identify potential unauthorized fraud but has a limited role in authorized push payment fraud
- As the AI/ML becomes more sophisticated, behavioral analyses will need to also advance to provide effective fraud mitigation. The effectiveness of behavioral analyses may weaken over time with the increased capabilities of AI/ML

See behavorial analysis country highlights from the UK

## Confirmation of Payee (CoP)

**Confirmation of Payee (CoP) is a limited, but helpful, tool to fight a subset of APP fraud.**

Confirmation-of-Payee is designed to help combat APP fraud by providing the sending party with the name associated with the receiving account prior to payment initiation. This helps stop misdirected payments (i.e., John from paying Mary, though he actually meant to pay Susan) while also preventing fraudsters from pretending to be someone or something (e.g., a government agency, business supplier) they are not (i.e., John convinces Mary that he is Susan, and Mary pays John believing she has paid Susan).

When CoP was first introduced in the UK it was not mandatory. As a result, fraudsters opened accounts at those institutions that did not support CoP and continued attacking victims.[6] CoP has been ineffective against account takeover (unauthorized fraud) or scams where the sender has been convinced to send money to the fraudster (authorized push payment fraud). It also requires sharing end user information to prove useful (i.e., first name is not enough, full legal names could lead to unwanted rejections).[7]

### Key takeaways

- CoP can prevent misdirected payments and APP fraud when the fraudster is pretending to be someone or something they are not
- CoP has not been effective in protecting against account takeover or scams where the sender has been convinced to send money to the fraudster
- Any CoP-like solution needs to have a consistent framework for participating financial institutions such as privacy, controls, and user experience

See Confirmation of Payee country highlights from the UK, the Netherlands, and Australia

# Technology

## Digital identity

**Digital identity (ID) is a key authentication technique for unauthorized fraud.**

Digital ID services enable end users to verify their identity in a digital-only environment. This can take many forms. Some governments enabled government-issued IDs usable in digital environments in the form of chips. Other markets embedded digital identity services into banking apps. Still others use bank-held information to verify consumer identities in digital environments such as online banking or payment initiation.

Digital IDs can form a key component of the Multi-Factor Authentication (MFA) or Strong Customer Authentication (SCA) process, limiting unauthorized fraud. This, however, implies that the digital ID itself is secure and accepted as a form of authentication for MFA/SCA purposes. Digital IDs need to combine security with usability as its utility will be limited if too difficult to use. Furthermore, digital IDs authenticate the sending party and verify that they have the authorization to initiate payments, making them ineffective for APP fraud.

### Key takeaways

- Digital IDs can form a key part of any MFA/SCA process
- Various players can create different sorts of digital IDs, including governments, financial institutions (using bank-held information), third party service providers, etc.
- Digital IDs need to strike a balance between security and ease of use
- Digital IDs can play a part in mitigating unauthorized fraud but have little impact with APP fraud

See digital identity country highlights from the Netherlands and Australia

# Scheme rules

## Limits and transaction holds

**Limits can lower fraudulent gains while transaction holds can provide FIs valuable time.**

Payment fraud can be minimized by using transaction and velocity limits and transaction holds.

Scheme rules typically establish an upper limit for a single transaction and participants have an option to set lower end user limits. These limits generally differ based on end user type and use case, and may vary based on sending or receiving payments. Velocity limits that restrict the number of transactions over a given period such as a day or week may also help to limit fraud losses.

Transaction holds provide participants (e.g., sending and receiving financial institutions) more time to analyze a transaction than is typically allowed by scheme rules. This can be tricky since transaction holds inherently impact the instant nature of instant payments. Transaction holds can be used against fraud, yet should only be used sparingly to limit the number of false positives and end user impact.

### Key takeaways

- Transaction limits can help prevent end users from substantial fraud losses
- Limiting the number of transactions over a given time can reduce losses from a single account
- Financial institutions should strike a balance of fraud-related holds and the end user impact

See limits and transaction holds highlights from the UK, the Netherlands and Brazil

## Enhanced authentication measures

**Strong Customer Authentication is another authentication tool to protect end users.**

Enhanced authentication measures (e.g., (MFA/SCA) authenticate transactions through multiple channels, helping to minimize unauthorized payment fraud. Typically, with MFA/SCA, multiple authentication factors need to be met, where it is something the end user:

- Knows (e.g., a password, PIN, or a secret question)
- Has (e.g., a token, smart card, or mobile device)
- Is (e.g., fingerprint, facial recognition, or voice recognition)

While MFA/SCA adds an extra layer of security for users, it also leads to some inconvenience. However, these may be considered smart friction and can help against unauthorized fraud. Authorized fraud, by definition, is not prevented by MFA because the authorizing party is authorized.

### Key takeaways

- MFA/SCA can be combined with cross-industry cooperation (i.e. against SIM swap fraud, where a new SIM card is connected to a user's mobile number on a new phone) to further strengthen unauthorized fraud protection measures
- MFA/SCA can be effective at preventing unauthorized payment fraud, although phishing, hacking, SIM swap fraud, etc. may be able to circumvent MFA measures

See enhanced authorization measures highlights from the UK, the Netherlands, Australia and Brazil

# Scheme rules

## Dispute resolution/loss recovery

**Common dispute resolution and loss recovery rules can protect financial institutions and consumers.**

A dispute resolution and loss recovery framework can support smooth resolution processes, liability transparency, and minimize fraud impact. There are typically three parts to dispute resolution mechanisms:

- Structured reporting channel that empowers end users to start resolution processes as early as possible
- Clear guidelines regarding liability that defines which entity holds the liability for authorized and unauthorized payment fraud
- Damage compensation mechanisms that provide clarity for end users when fraud does take place

The framework should employ an open and transparent common user experience to avoid dispute resolution processes as a point of competition among financial institutions and friction for end users.

### Key takeaways

- Clear and consistent guidelines for dispute resolution should address reporting, loss recovery and liability
- None of these efforts will prevent authorized or unauthorized payment fraud per se. However, establishing a framework can help incentivize all payment participants to do their part to reduce fraud

See dispute resolution/loss recovery highlights from the UK, Australia and Brazil

# Awareness

## End user education

**End users can be one of the weakest links; education is key to limiting all types of fraud.**

End user education is an important way for the financial services community to alert end users about common types of fraud being perpetrated. Other industry players, such as the scheme or system operators, can also play a part in sharing information and insights with the wider industry, creating a feedback loop for payments participants.

End user education should be a continuing exercise that is periodically updated to include the latest information on scams, fraud types, and industry best practices to identify fraud attempts and protect oneself.

### Key takeaways

- Fraud education needs to be ongoing and periodically updated to reflect current trends and new tools or techniques used by fraudsters
- As the main contact for payments end users, financial institutions need to play a leading role in anti-fraud education
- Other players, such as scheme or system operators and payment processors, need to participate in feedback loops so that information can be widely shared within the payments industry

See end user education highlights from the UK and the Netherlands

## Fraudulent individual database

**Increased amounts of information-sharing among system participants can help prevent further fraud.**

Fraudulent individual databases help participants identify suspicious aliases, bank accounts, or identities used to commit fraud. These databases can be maintained by a number of entities, including the central infrastructure, government, industry associations, or financial institutions.

In some markets participants can access the database to enhance their fraud prevention systems, report aliases or accounts used for fraud, and alert other participants to minimize fraud. In other markets these databases are used to prevent fraudsters from opening bank accounts, thereby reducing the fraudsters' ability to open new accounts at different financial institutions.

Any database and data usage practice needs to ensure compliance with privacy regulations.

### Key takeaways

- A fraudulent individual database is one way to allow financial institutions to check transactions against existing information prior to a payment being sent to mitigate unauthorized payment fraud
- Financial institutions can flag an alias or proxy in a centralized database to warn end users about flagged proxies prior to sending a payment. This approach is best to use as a supplement to other solutions to reduce authorized push payment fraud

See fraudulent individual database highlights from the UK, Brazil and the Netherlands

# Awareness

## Cross-industry collaboration

**Widespread industry collaboration is critical – fraud should not be a competitive issue for any party.**

Cross-industry collaboration at the community level helps mitigate fraud. This includes information-sharing and awareness campaigns, as well as cross-industry cooperation with telecommunications companies coordinating with the banking industry to prevent authorized push payment fraud. Other examples include cooperation with law enforcement or information-sharing in industry associations.

### Key takeaway

- There are many ways in which the community needs to cooperate, both within and outside of the payments ecosystem

See cross-industry collaboration highlights from the UK, Australia and the Netherlands

# 04 Conclusion

## While the future cannot be predicted, the North America market can prepare for it

### Stay abreast of global fraud trends

Fraudsters are getting smarter. They are agile, search for weaknesses across the payments value chain and operate without regard to geographic boundaries. As a result, scams and frauds used in other geographies are likely to be adapted to the North America market.

### Get started and adapt to changing needs

The technology is rapidly evolving. AI/ML affords fraudsters a new sophisticated toolset using chatbots and deep fakes, thereby creating new challenges for the financial community. Retrofitting technology, particularly when instant payments need to be achieved within milliseconds, can be expensive and time consuming for key stakeholders. The North America market can benefit from applying learnings to their risk mitigation strategies and establishing a fraud mitigation roadmap that continuously adapts to threats.

### Build trust and confidence

End users need more education and tools to protect themselves from being victimized as instant payments adoption increases. At the same time, end users may expect their financial institutions and key stakeholders to protect them.

Regulators and scheme operators in other countries are clarifying responsibilities for fraud. The North America market will likely evolve to provide consumer protections beyond what exists today.

### Innovate to achieve a whole that is greater than the sum of its parts

No individual stakeholder can prevent instant payments fraud. The instant payment stakeholders have a key role in providing the visibility needed to identify and mitigate fraud. Fraud controls at the financial institution with centralized monitoring at the scheme level, can strengthen the entire ecosystem.

## The time to act is now

# 05 Country-specific highlights

## Technology

### Fraud monitoring system

UP

The use of fraud scoring at the central infrastructure level provides insights to sending and receiving financial institutions.

Country capsule:
**United Kingdom**

The Mule Insights Tactical Solution (MITS) was developed to combat money laundering and usage of mule accounts by analyzing transaction data post processing and identifying patterns that indicate potential money mule activity. The tool uses machine learning algorithms to identify anomalies in transaction patterns for processed transactions such as a sudden increase in the number or value of transactions, or transactions involving accounts that have no apparent connection to each other.

When MITS identifies suspicious activity, it alerts bank investigators, who can then investigate the activity further and take appropriate action. This allows financial institutions to identify potential money mule activity and freeze accounts or block future transactions. The tool can be integrated into other fraud detection and prevention tools. MITS does not monitor possible fraudulent transactions, as it captures and analyzes transcations after they have been processed.

Country capsule:
**Brazil**

Pix participants have anti-fraud engines that detect atypical transactions according to the user's profile and block suspicious transactions for up to 30 minutes during the day or 60 minutes at night. Transactions can be rejected and marked as suspicious if fraud is suspected.[8]

Participants must provide feedback on fraud cases to alert participants of the aliases used to commit fraud.

# Technology

## Biometric tools

APP UP

The use of biometrics (e.g., fingerprint, iris scan, facial recognition) to authenticate users prior to sending a payment.

### Country capsule: **United Kingdom**

Europe's PSD2 added three types of authentication methods for payments, one of which involves the use of biometrics such as fingerprints and facial ID.[9] Some UK financial institutions use voice biometrics to compare the caller's voice with the voiceprint stored in their database to ensure that the caller is who they claim to be.

### Country capsule: **The Netherlands**

The Netherlands incorporated the use of biometric tools for fraud prevention in its enhanced authentication process for payments. As part of PSD2's SCA regulations, users need to fulfill two of three potential authentication methods: something you know (password, PIN), something you have (device), or something you are (biometrics such as facial ID or fingerprint).[10]

### Country capsule: **Australia**

In addition to using a combination of biometric tools like fingerprints for customer authentication, some banks allow end users to utilize Voice ID instead of a PIN or password. Voice ID is a unique, encrypted voiceprint created through a phone conversation. For example, an end user wishing to make a payment over a specified amount would verify themselves by saying a phrase such as “My voice confirms my identity.”

### Country capsule: **Brazil**

Pix users utilize biometric tools to authenticate themselves when initiating payments, including facial ID and fingerprints.[11]

# Technology

## Behavioral analysis

APP UP

The use of data to categorize and analyze user-level behavior and identify anomalies in either payment information (i.e. sending payments to an unknown person or entity) or in the user's usage of the service (i.e. incorrect PIN input, abnormal location data, unusual time of initiation).

### Country capsule: **United Kingdom**

Some UK financial institutions utilize environment detection technology to detect if the caller is calling from an environment that is not their usual one, such as using a different phone.

When an end user logs into its financial institution, thousands of movements are recorded from the keyboard, mobile app, and/or website. On a smartphone, software measures the angle at which the device is held, which fingers are used to swipe/tap, and how hard or light pressure is applied. On a computer, the software collects data on the rhythm of the keystrokes and how the mouse is used. This enables the financial institution to create a user profile to compare against future actions. Potential fraud can be flagged when values in the end user's profile differ substantially from the norm.

# Technology

## Confirmation of Payee (CoP)

APP

The ability for the sender to confirm the name related to the receiver's alias or account information prior to sending a payment.

### Country capsule: **The Netherlands**

The International Bank Account Number (IBAN) Name Check is a joint initiative where a sender can confirm the receiver by entering their IBAN and name. When the name-check result is erroneous, the sender receives a warning notification. If the name entered is similar but incorrect, the sender receives a name suggestion meant to reconfirm the information.

Nonetheless, end users remain responsible for how they respond to the warning. The service only operates for transfers conducted via online or mobile banking. It has reportedly helped mitigate misdirected payments by 67% in the Netherlands since its development in 2017.[12]

### Country capsule: **United Kingdom**

CoP was introduced in the UK in June 2020 by six of the UK's largest financial institutions and is now mandatory. What originally involved Barclays, HSBC, Lloyds, Nationwide, RBS, and Santander now includes an additional 59 voluntary adherents. An additional ~400 financial organizations were directed by the Payment Systems Regulator (PSR) to implement CoP by October 2024.[13]

Pay.UK sets guidelines and requires its participants to use clear warning messages if senders choose to proceed with the payment despite having received a negative CoP response.[14] This is to ensure that senders are aware that they are potentially making a payment to a different receiver than they originally had intended.

# Technology

## Confirmation of Payee (CoP)

APP

The ability for the sender to confirm the name related to the receiver's alias or account information prior to sending a payment.

### Country capsule: **Australia**

PayID provides a CoP-like function, permitting end users to register their phone number, email address, Australian Business Number (ABN), or a display number in a central repository.[15] These aliases can be used to directly receive and initiate payments. Transactions made via PayID are processed after the sender elects to check the name associated with the beneficiary's account.

Participating institutions need to:

- Ensure the alias name reasonably and accurately represents the name of the account holder and conduct rigorous verification steps to promote confidence
- Disable and de-register any alias identifier associated with an account that the participant reasonably suspects to have been used for fraudulent purposes
- Monitor any misuse of the PayID service and have controls in place such as automated lock outs when unusual activity is detected

# Technology

## Digital identity

UP

The use of a secure digital ID to verify the sender's identity.

### Country capsule: **Australia**

The Australian Payments Council (APC) is developing a TrustID Framework, administered by an Australian Payments Network (AusPayNet) working group, to create standards around secure data-sharing and authentication for digital identity.[16] Australia is also awaiting the roll-out of its digital identity exchange in 2023, ConnectID. ConnectID is government accredited and operates as an intermediary between independent identity service providers. Identity providers store consumer identities and take responsibility for providing the secure information only under the consent of the identity owner. The end user controls who receives and uses their identity data.[17,18]

An executive agency of the Australian Government plans to integrate the government's digital identity system in support of government benefit payments or apply for services.[19]

### Country capsule: **The Netherlands**

iDIN is a Dutch identity scheme that allows users to identify themselves online using their financial institution log-in information or to confirm their identity and age. iDIN provides Dutch citizens with a safe authentication method for banking services that can be used for other purposes (e.g., insurance). iDIN services utilize bank-held information to provide "identity-as-a-service".[20]

# Scheme rules

## Limits and transaction holds

APP UP

The option to define limits and hold times such as:

- Transaction value limits: Value limits for individual transaction or during certain time windows
- Velocity limits: Daily, weekly, monthly limits on the number of payments sent or received
- Transaction holds for analysis: Rules that enable participants to conduct more detailed fraud analysis on transactions despite standard scheme service level (SLA) requirements

### Country capsule: **United Kingdom**

The Faster Payments System (FPS) transaction value limit has increased significantly, starting at GBP 1,000 in 2008 and currently standing at 1 million. FPS publishes the transaction limits for personal and business accounts and the type of transaction (e.g., one-off, standing order) for each financial institution.[21] Some financial institutions may also enforce velocity limits. Financial institutions started with low transaction limits that were increased over time.

### Country capsule: **The Netherlands**

Instant Payments Clearing and Settlement Mechanism (IP CSM) imposes no value limit for domestic payment transactions. The European Payments Council established a maximum amount for cross-border intra-SEPA payments of EUR 100,000.[22]

### Country capsule: **Brazil**

Brazil Central Bank imposed a BRL 1,000 transaction limit from 8 pm to 6 am to combat "lightning kidnappings", where victims were abducted and not released until a real time payment was initiated to the captors.[23] Financial institutions can increase this limit after a minimum wait time or customized upon customer request. This value limit is expected to be effective in mitigating scams and fraud without jeopardizing Pix's utility because the average Pix transaction is under BRL 500.

# Scheme rules

## Enhanced authentication measure

UP

The use of an extra layer of security to authenticate the end user (e.g., SCA/MFA).

### Country capsule: **United Kingdom**

The UK introduced SCA regulations in September 2019 as part of the EU's Revised Payment Services Directive (PSD2).[24] Under SCA regulations, payment service providers (PSPs) need to implement multi-factor authentication for some online payments, such as high-risk and high-value transactions. The authentication process needs to be performed in real-time and be designed to prevent fraud and unauthorized access to the user's account.

### Country capsule: **Australia**

Australian financial institutions employ a combination of multi-factor authentication and biometrics, such as fingerprint and voice, that comply with the Guiding Principles for Accessible Authentication developed by the Australian Banking Association (ABA).[25]

### Country capsule: **Brazil**

Each Pix participant needs to ensure secure customer authentication. The Brazilian Central Bank recommends the use of MFA mechanisms, including biometrics.[26] Pix participants can choose the specific customer authentication methods for Pix transactions, though many utilize biometrics.

### Country capsule: **The Netherlands**

The 2019 Revised Payment Service Directive (PSD2), as well as the Financial Supervision Act and Dutch Civil Code, enforce SCA requirements.[27]

# Scheme rules

## Dispute resolution/loss recovery

APP UP

The use of rules or regulations regarding fraud resolution and loss recovery for consumer protection purposes.

### Country capsule: **United Kingdom**

The Contingent Reimbursement Model (CRM) Code is a voluntary industry code designed under the PSR and implemented to provide greater protection to consumers, micro-businesses, and small charities against APP scams.[28] With CRM, the financial institution or PSP reimburses the end user for their losses if they meet the standards set in the code. Effective January 2024, the liability will be equally borne by the sending and receiving financial institutions.

The Lending Standards Board (LSB), a regulatory body, monitors the CRM Code's effectiveness in reducing the number of APP scams.[29] And there is a Financial Ombudsman Service to assist with dispute resolution between end users and financial institutions on decisions made under the Code.[30]

### Country capsule: **Brazil**

Pix adopted a Special Return Mechanism, allowing senders to initiate a refund process under two circumstances: (1) well-founded suspicion of the use of Pix in a fraudulent way or (2) operational failure in the information technology system of any of the participants in the transaction.[31] This is designed to provide end users with more control in the fraud resolution process and increase cooperation with receiving institutions in returning funds in admitted cases.

### Country capsule: **Australia**

Many Australian financial institutions subscribe to the voluntary ePayment Code of Conduct, which requires subscribers to give end users clear and unambiguous terms and conditions regarding electronic payments and online banking.[32] Financial institutions are liable to compensate end users in the event of any fraud loss that occurs because of erroneous PayID registration.

# Awareness

## End user education

APP UP

The efforts to educate end users to make them aware of safety and precautions that may protect against payment fraud (e.g., campaigns such as "Take Five to Stop Fraud").

### Country capsule: **United Kingdom**

Fraud prevention initiatives in the UK, such as "Don't Be Fooled" and "Take Five to Stop Fraud," are aimed at educating customers about common types of fraud and how to protect themselves from falling victim to fraudsters. These initiatives are backed by the Take Five Charter, a voluntary code of conduct signed by many banks and building societies.

"Don't Be Fooled" is a public awareness campaign in collaboration with UK Finance and Cifas, a non-profit organization, aimed at young people who are frequently targeted to act as money mules.[33] "Take Five to Stop Fraud" is a national campaign that encourages people to take five minutes to stop and think before rushing into responding to unexpected requests for personal or financial information.[34]

Banks and police collaborate on the Banking Protocol to fight fraud by training bank branch staff to recognize signs of scams and alert law enforcement.[35]

### Country capsule: **The Netherlands**

The Dutch payments industry supports the "Secure Banking Website" as the main channel to inform customers about fraud and security, and how consumers themselves can contribute to fraud prevention.[36] The industry has developed five security steps for end users to follow to prevent fraud, including keeping security codes secret and immediately reporting incidents using the financial institution's instructions.

Every year the Netherlands holds a Fraud Film Festival for the general public to increase awareness, which showcases fraud in industries beyond the financial sector.[37]

# Awareness

## Fraudulent individual database

APP UP

The use of a database to share fraud-related data across multiple parties, particularly on known fraudsters.

### Country capsule: **The Netherlands**

Financial institutions share certain customer data among themselves to reduce the risk of financial fraud through a joint warning system called the External Referral Register (EVR).[38] Reference details (name and date of birth) of persons who have committed fraud or who have attempted to do so are registered within the EVR.

Authorized financial institution employees have limited access to information. When performing a check in the EVR, the employee only sees whether an entry has been made in the register. Detailed information (e.g., reason for being listed) is excluded for privacy and compliance purposes.

A sending financial institution can exchange suspected fraud messages using an ISO 20022 message. The receiving financial institution can use this information, such as combining it with its own internal scoring, to assess whether further investigation is warranted.[39]

### Country capsule: **Brazil**

The Pix central infrastructure maintains a fraud database, enabling participants access to enhance their fraud prevention systems, report aliases or accounts used for fraud, and alert other participants to minimize fraud. Pix scam or fraud victims can file a complaint with the receiving financial institution and/or where the proxy was used.[40] Financial institutions use this information to report accounts and proxies associated with payments fraud.[41] The proxies marked as fraud are shared with all participants. Alerts are sent whenever the fraudulent proxy is used.

### Country capsule: **United Kingdom**

Pay.UK and UK Finance collaborated to create the Enhanced Fraud Data Standards Group (EFDSG). The EFDSG developed a new tool called the "logical data model" to help fight APP fraud by categorizing relevant customer data that enables banks to easily identify fraudulent transactions.[42]

Financial institutions share data via an open API, allowing more complete risk-scoring prior to payment initiation.

# Awareness

## Cross-industry collaboration

APP UP

The use of cross-industry collaboration to collectively address fraud mitigation (e.g., financial servces, law enforcement, telcos).

### Country capsule: **United Kingdom**

The UK has many examples of industry collaboration including the Dedicated Card and Payment CrimeUnit.[43] This specialist police unit targets organized criminal groups accountable for financial fraud and scams. Financial institutions and the police collaborate by training bank branch staff to identify signs of scams and alert law enforcement.

UK Finance and the communications regulator, Ofcom, created the Do Not Originate (DNO) list to protect legitimate numbers by recording telephone numbers that are used by organizations exclusively for receiving incoming calls.[44] The DNO list is shared with telecom providers to identify and block calls, as well as with some call blocking and filtering service providers.

### Country capsule: **Australia**

Australia created several entities including the ReportCyber (formerly ACORN, the Cybercrime Online Reporting Network operated by the Australian Cyber Security Centre (ACSC)), the Scams Awareness Network (SAN), the Economic Crime Forum (ECF) and Australian Financial Crime Exchange (AFCX) to increase awareness on fraud detection and mitigation, and encourage industry cooperation.[45,46,47] The Australian Competition & Consumer Commission (ACCC), for instance, shares scam reports with the AFCX for provision of real-time fraud information.[48]

### Country capsule: **The Netherlands**

Dutch Payment Association (DPA) members set up the Payment Institutions – Information Sharing and Analysis Centre (PI-ISAC) to exchange information on fraud, threats, cyber safety, and best anti-fraud practices between participants.[49]

Twice a year, the National Forum of Payment Systems (NFPS) takes place to discuss issues surrounding the Dutch Payment System such as security, efficiency, and availability.[50]

# 06 Glossary

| | |
|---|---|
| ABA | Australian Banking Association |
| ABN | Australian Business Number |
| ACCC | Australian Competition & Consumer Commission |
| ACSC | Australian Cyber Security Centre |
| ACFT | Australian Financial Crime Exchange |
| ACORN | Australian Cybercrime Online Reporting Network (now ReportCyber) |
| AFCX | Australian Financial Crime Exchange |
| AI/ML | Artificial Intelligence / Machine Learning |
| AML | Anti-money laundering |
| APC | Australian Payments Council |
| APP | Authorized Push Payment Fraud |
| ATM | Automated Teller Machine |
| AUD | Australian Dollar |
| B2B | Business-to-Business |
| BCB | Banco Central do Brasil |
| BRL | Brazilian Real |
| CI | Central Infrastructure |
| CIP | Câmara Interbancária de Pagamentos |
| CoP | Confirmation-of-Payee |
| CRM | Contingent Reimbursement Model |
| CSM | Clearing and Settlement Mechanisms |
| DNO | Do Not Originate list |
| DPA | Dutch Payments Association |
| EFDSG | Enhanced Fraud Data Standards Group |
| EPC | European Payments Council |
| EVR | External Referral Register |
| FBF | Fraud Banking Forum |
| FI | Financial Institution |
| FI-ISAC | Financial Institutions – Information Sharing and Analysis Center |
| FPS | Faster Payments System |
| GBP | British Pound |
| IBAN | International Bank Account Number |
| iDIN | Dutch digital ID service |
| IP CSM | Instant Payments Clearing and Settlement Mechanism |

# Glossary

| | |
|---|---|
| **MFA/SCA** | Multi-Factor Authentication/Strong Customer Authentication |
| **MITS** | Mule Insights Tactical Solution |
| **NFPS** | National Forum of Payment Systems |
| **P2P** | Peer-to-peer |
| **PI-ISAC** | Payment Institutions – Information Sharing and Analysis Centre |
| **PIN** | Personal Identification Number |
| **PSD2** | The Europe Revised Payment Services Directive |
| **PSP** | Payment Service Provider |
| **PSR** | Payment Systems Regulator |
| **RTR** | Real-Time Rail (Canada) |
| **SCA** | Strong Customer Authentication |
| **SIM** | Subscriber Identity Module (mobile phone memory card) |
| **SLA** | Service Level Agreement |
| **UK** | United Kingdom |
| **UP** | Unauthorized Payment Fraud |
| **USD** | US Dollar |

# 07 Endnotes

1. UK Finance Annual Fraud Report 2022. https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf
2. Ibid.
3. UK Annual Fraud Report 2022. https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf
4. https://www.scamwatch.gov.au/research-and-resources/scam-statistics
5. https://www.ukfinance.org.uk/news-and-insight/blogs/confirmation-payee-journey-so-far
6. https://www.ukfinance.org.uk/policy-and-guidance/guidance/confirmation-payee#:~:
7. https://www.bcb.gov.br/en/financialstability/pixfaqen
8. https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5620
9. https://zoek.officielebekendmakingen.nl/stb-2018-503.html
10. https://www.bcb.gov.br/en/financialstability/pixfaqen
11. https://thebankingscene.com/opinions/iban-name-check-lessons-learned-from-the-uk-and-the-netherlands
12. https://www.psr.org.uk/news-and-updates/latest-news/news/psr-directs-400-firms-to-introduce-the-payment-protection-measure-confirmation-of-payee/
13. https://www.ukfinance.org.uk/policy-and-guidance/guidance/confirmation-payee
14. https://payid.com.au/
15. https://www.auspaynet.com.au/insights/consultations/TrustID2020
16. https://connectid.com.au/#:~:text=ConnectID%20is%20an%20Australian%2Downed%20and%20operated%20digital%20identity%20solution,to%20securely%20verify%20their%20identity
17. https://www.digitalidentity.gov.au/news/eftpos-accreditation-annual-assessment-a-success#:~:text=While%20ConnectID%20securely%20facilitates%20the,consent%20of%20the%20identity%20owner
18. https://www.digitalidentity.gov.au/sites/default/files/2021-11/Digital%20Identity%20Legislation%20-%20what%20is%20it%20-%20factsheet.pdf
19. https://www.idin.nl/en/
20. https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/transaction-limits/
21. https://www.europeanpaymentscouncil.eu/what-we-do/sepa-instant-credit-transfer
22. https://www.pymnts.com/news/international/2021/brazil-limits-pix-payments-amid-kidnapping-spree/
23. https://www.fca.org.uk/firms/strong-customer-authentication
24. https://www.ausbanking.org.au/wp-content/uploads/2019/05/Accessibility_Principles_for_Banking_web.pdf
25. https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=1

# Endnotes

26. http://www.dutchcivillaw.com/legislation/dcctitle7777bb.htm
27. https://www.psr.org.uk/our-work/app-scams/#:~:text=The%20Contingent%20Reimbursement%20Model%20(CRM)%20Code&text=It%20sets%20out%20standards%20for,ten%20signatories%20to%20the%20Code
28. https://www.lendingstandardsboard.org.uk/resources/why-the-crm-codes-protections-are-here-to-stay/
29. https://www.financial-ombudsman.org.uk/
30. https://www.bcb.gov.br/en/financialstability/pix_en
31. https://download.asic.gov.au/media/lloeicwb/epayments-code-published-02-june-2022.pdf
32. https://www.moneymules.co.uk/
33. https://www.takefive-stopfraud.org.uk/
34. https://www.ukfinance.org.uk/news-and-insight/blogs/why-banking-protocol-matters
35. https://www.veiligbankieren.nl/
36. https://www.fraudefilmfestival.nl/en/
37. https://www.verzekeraars.nl/media/9002/protocol-incidentenwaarschuwingssysteem-financi%C3%ABle-instellingen-pifi-2021-eng_.pdf
38. https://www.betaalvereniging.nl/wp-content/uploads/How-to-keep-payments-safe-and-secure-Marco-Doeland.pdf
39. https://www.bcb.gov.br/en/financialstability/pix_en
40. https://www.bcb.gov.br/en/publications/our_results_2021
41. https://newseventsinsights.wearepay.uk/media-centre/press-releases/payuk-and-uk-finance-publish-first-iteration-of-technical-collateral-for-enhanced-fraud-data-standard/
42. https://www.ukfinance.org.uk/dedicated-card-and-payment-crime-unit
43. https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-scam-calls-and-texts/do-not-originate
44. https://www.cyber.gov.au/about-us/privacy
45. https://www.scamnet.wa.gov.au/scamnet/About_us-Scams_Awareness_Network.htm
46. https://auspaynet.com.au/network/economic-crime-forum
47. https://www.afcx.com.au/
48. Annual Report 2022, Dutch Payments Association. https://www.betaalvereniging.nl/en/latest-news/publications/
49. https://www.dnb.nl/en/inclusive-society/national-forum-on-the-payment-system/

# 08

# About

## About Visa

Visa (NYSE: V) is a world leader in digital payments, facilitating transactions between consumers, merchants, financial institutions and government entities across more than 200 countries and territories each year. Our mission is to connect the world through the most innovative, convenient, reliable and secure payments network, enabling individuals, businesses and economies to thrive. We believe economies that include everyone everywhere, uplift everyone everywhere and see access as foundational to the future of money movement. Learn more at Visa.com.

Visa has decades of experience providing value-added services for card-based payments. Our global expertise also supports instant payments use cases spanning the transaction lifecycle.

## About Lipis Advisors

Lipis Advisors is Berlin-based consultancy focused exclusively on the payments industry. We serve banks, payment processors, technology providers, fintechs, investors, and government regulators on a number of topics including payment strategy, product development, functionality benchmarking, and education. Our highly sought international team works with some of the world's largest payment companies and regularly speaks at industry events all over the world.

All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.