

**A Finextra Research report
in association with LexisNexis® Risk Solutions
February 2025**



CONFIRMATION OF PAYEE PROGRESS AND APP FRAUD MITIGATION: WHERE ARE WE NOW?

EMEA vs. APAC vs. North America

Finextra®

01	Introduction	3
02	Europe, Middle East and Africa	7
03	Asia Pacific.....	14
04	North America	20
05	Conclusion.....	25
06	About.....	26

Introduction




This report compares Confirmation of Payee progress and APP fraud mitigation across EMEA, APAC and North America, and features expert commentary from AccessPay, Bottomline, Finastra and NatWest.

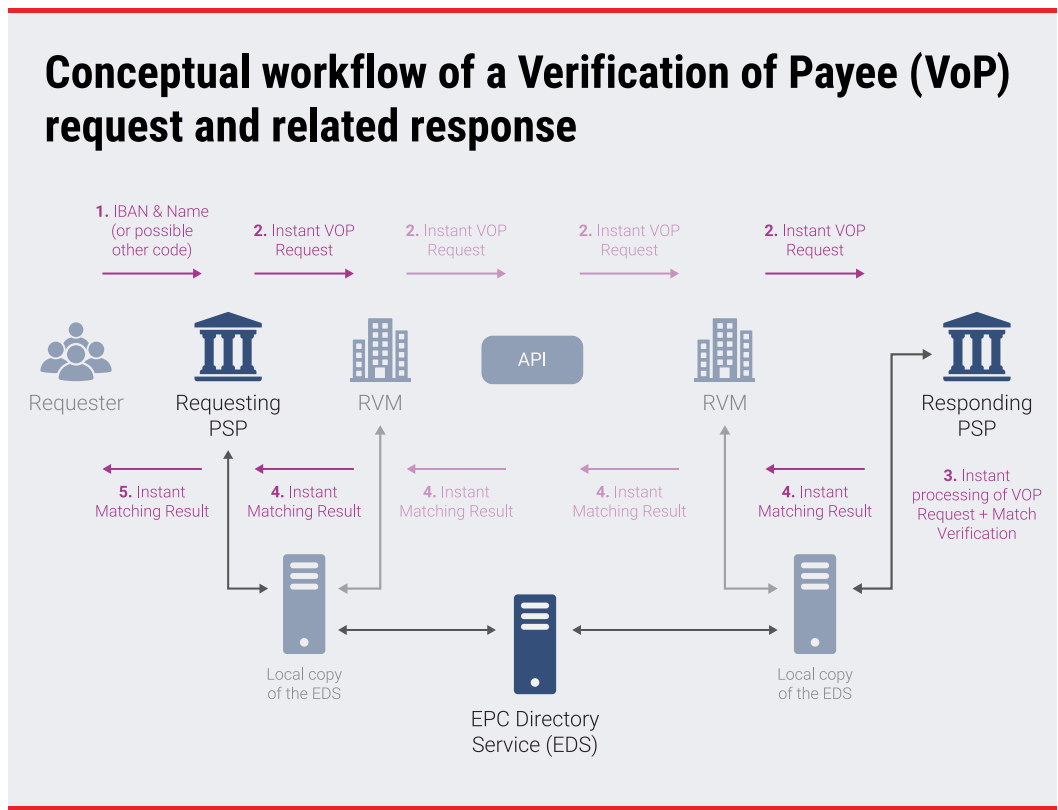
When a payment instruction is created for a company or by an individual, the bank account name, sort code, account number and the beneficiary's name is required. While it is assumed that this identifying information is checked before the payment goes through, today, this assumption is not sufficient. That's because the type of payment scam where people are contacted by fraudsters and asked to transfer funds to a new account in their name – known as Authorised Push Payment (APP) fraud – is prevalent and growing.

Using the UK as the blueprint for success, the 2015 Pay.UK report on enhancing the payments experience drew a line in the sand and outlined a path forward for improvement and innovation across payment infrastructure. At the time, a key action for Pay.UK was to establish a three-way match between the beneficiary name, sort code and bank account number. Beyond the benefits for fraud mitigation, this also decreased the chances of funds being sent to the wrong individual or organisation and hoping that the money would be repaid.

Confirmation of Payee (CoP) – as an idea – was born. For individuals and companies setting up new payees and payments, the aim was for payment providers to be able to confirm the name provided with the account name.

The Association of Corporate Treasurers outlined the outcomes of CoP:

- 
Yes - If the correct account name is used, confirmation that the details match is sent, and the payment is completed.
- 
No, please check - If a similar name to the account holder is used, the actual name of the account holder is provided so it can be confirmed. The details can be updated and the payment can be attempted again.
- 
No, the name is wrong - If the wrong name for the account holder is entered, the payee will be told the details do not match and advised to contact the person or organisation they are trying to pay.

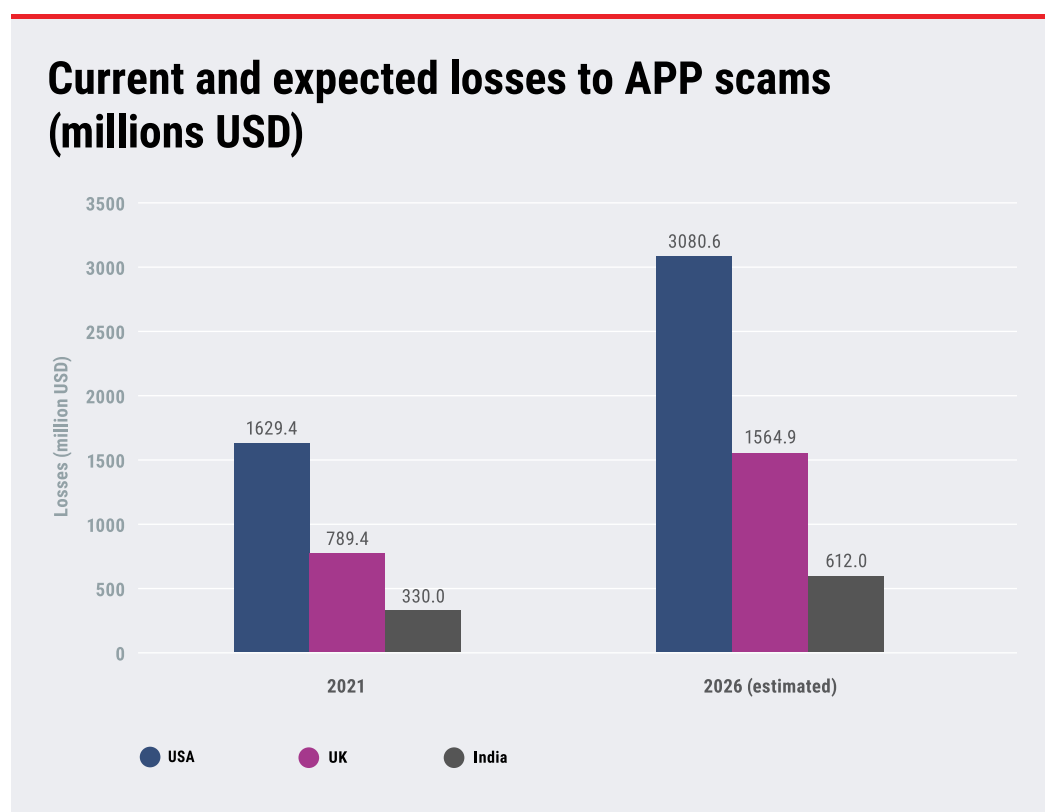


Source: [European Payments Council](#)

Because the outcomes are numerous, the way in which verification was first established adds friction to the customer payments journey. Seamless processes and transparent communication is the best way forward, and that came to the fore with the Contingent Reimbursement Model (CRM), which provides payers that have received a positive match greater protection from financial losses if they have been APP fraud victims. In 2019, consumers that received a partial match or no match were not eligible for this.

However, with the continued focus on mitigating the increasing levels of APP fraud, in 2023, CRM changed from being voluntary to financial institutions being mandated to instil processes that would review accounts that had been identified as being at higher risk of being used to facilitate APP fraud or misdirected payments. Alongside this, firms were tasked with establishing processes to profile inbound payments so that funds that were suspected of being credits to an account and were the proceeds of an APP fraud scam were prevented from being moved.

Moreover, failure to meet these requirements will impact an institution's ability to rely on exceptions provided in the CRM Code regarding reimbursing customers who are victims of APP fraud. From October 2024, the Payment System Regulator (PSR) has started to enforce banks and payment service providers (PSPs) to reimburse victims of payment scams. While the UK is leading in this endeavour, it is evident that the rest of Europe, the Middle East, Africa, Asia Pacific and North America is and will follow suit.



Source: ACI Worldwide – an overview of estimated losses to APP scams in the UK, India and the US.

The impact of these developments will be substantial. APP fraud losses are expected to double across EMEA, APAC and North America, and legislation mandating CoP on a national or regional basis must be established across the globe. It is estimated that APP fraud losses in the UK, India and the UK will hit \$5.25 billion, with a CAGR (Compound Annual Growth Rate) of 21% across the 2022-2026 period, according to an **ACI Worldwide and GlobalData report**. Action must be taken, and if regulations are not put in place, financial institutions and PSPs must ensure they are leveraging technology solutions to bolster verification mechanisms themselves.

Striking the balance between protecting the end customers, adding minimal friction to processes, and assessing fraud prevention procedures will be a cumbersome, yet important, project. This report, explores how to meet that need, how success stories in EMEA will set the trend for other regions, the impact non-CoP initiation in APAC will have on international payments and what the future holds for technology solutions that can detect account activity in North America.

02

Europe, Middle East and Africa

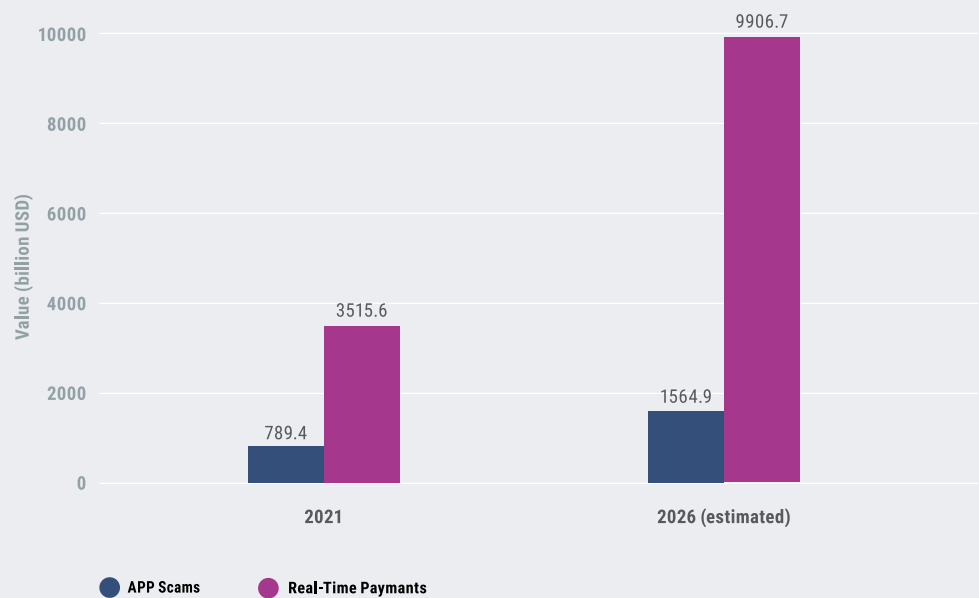
What is the state of play for APP fraud and misdirected payment fraud across EMEA?

Erez Nounou, product lead risk solutions – financial messaging, Bottomline, highlights that while the “landscape of payment fraud prevention in the EMEA region is rapidly evolving [...] significant strides are being made in the implementation of pre-verification tools like Confirmation of Payee (CoP) and Verification of Payee (VoP). “These tools are integral in mitigating fraud by allowing pre-validation of payment details, thereby reducing the risk of fraudulent and misdirected transactions,” he continues.

UK

APP fraud has been an increasing concern for both banks and customers. Consumer education and fraud prevention are being prioritised by financial institutions, but regulators are questioning liability and reimbursement. With **UK Finance** research revealing that consumers lost £570 million to scams in the first half of 2024, and APP fraud accounting for over £213 million of that figure, a sea change will need to emerge to make an impact. CoP could be that solution.

Growth of APP scams vs. real-time payments (billions USD)



Source: ACI Worldwide – an overview of growth of APP scams in comparison to real-time payments in the UK.

UK Finance data on APP fraud in H1 2024 shows:

- 97,344 was the total number of APP fraud cases.
- £213.7 million was the total lost to APP fraud, comprising over £165.5 million of personal losses and over £47.2 million of business losses.
- 72% of APP fraud cases originated from online sources. These cases include lower-value scams, such as purchase scams, and account for 32% of total losses.
- 16% of cases originated in telecommunications and these include higher value cases, such as impersonation fraud, and account for 35% of total losses.

As UK banks significantly invested in increasing efforts to warn customers of scams:

- The number of fraud cases where criminals impersonate a bank or the police and convince someone to transfer money to a “safe account” fell by 32%.
- The number of purchase scams, where a victim pays in advance for products or services they never receive, fell by 11%.
- The number of romance scams fell by 7%.
- The number of investment scams fell by 29%.

Additionally, £126.7 million of APP losses was returned to victims, equating to 59% of the total loss. New reimbursement rules from the PSR came into effect on 7 October 2024, meaning that sending and receiving banks are now responsible to split reimbursements 50:50.

SEPA region

European regulators also recognise the need to address APP fraud. At the end of 2024, **EBA Clearing’s** pan-European VoP feature launched, which supports providers by offering IBAN name matching services to their customers for SEPA transactions. PSPs will be required to offer such services to payers from October 2025 onwards, as mandated by the new Instant Payments Regulation. With the PSR and PSD3 focused on tackling fraud that relies on manipulative techniques, like APP fraud, CoP processes will need to be seamless to be compliant by 2026/2027.

Sean Moriarty, CFO, AccessPay, explains that this will require “banks to confirm the name provided for the payment recipient matches the actual name registered for that IBAN before allowing transfers. Implementing comprehensive IBAN verification is challenging due to the lack of a centralised IBAN-name database across Europe. Some countries have local solutions, but there is no pan-European system yet. Meeting PSD3’s tight 2025 deadline may also be difficult for banks running on legacy technology not built for high volume real-time IBAN queries.”

He adds: “No single initiative can solve payment fraud alone, but layering technological safeguards like IBAN checks with process improvements and advanced fraud detection analytics should collectively help financial institutions get better control over domestic and international payment fraud risks across the EMEA region over time.”

Middle East

APP fraud, namely bogus phone calls, are daily occurrences in the Middle East. It is also cumbersome to gauge how many attempts are successful because cases can take months to investigate. This is a cultural issue, because often companies and individuals do not want to publicise their weaknesses.

An **AGBI** article reveals that:

- 50,000 cyberattacks a day, from ransomware to cyberterrorism, are thwarted, according to Mohamed Al Kuwaiti, head of cybersecurity for the UAE government.
- 32% of chief information security officers have seen an increase in targeted attacks in 2023, according to Eastnets.
- 1 in 11 applications to open new accounts turn out to be fraudulent, as found by LexisNexis® Risk Solutions.
- 41% of cyberattacks on organisations in the Middle East involve social engineering techniques such as psychological manipulation, as seen in phishing emails or calls from ‘your bank’ trying to scare and/or rush consumers into giving out information or transferring money.

Africa

APP fraud is also prevalent in Africa, where get-rich-quick investment scams are popular and seem like attractive offers due to scammers making an extra effort to be perceived legitimate and opening bank accounts with names similar to recognisable brands.

FICO data reveals that:

- 64% said they knew of someone that had been a victim of a scam.
- 19% said they had paid for investments, goods or services they never received.
- 56% of consumers think they are ultimately responsible if they send a payment to a scammer.
- 15% would change banks if they were a scam victim and were not satisfied with the bank’s response.
- 29% said they think a bank should always refund a scam victim, while 38% think they should be refunded most of the time.

Which countries/regions have implemented CoP within EMEA?



United Kingdom: LIVE – At the forefront of implementing CoP and the system has significantly contributed to reducing APP fraud.



The Netherlands: LIVE – Adopted CoP-like mechanisms to enhance payment security, focusing on pre-validation checks.



Belgium: LIVE – Adopting CoP mechanisms, driven by the need to enhance payment fraud prevention.



United Arab Emirates: ALTERNATIVE – **verification requirements** are in place only for cross-border payments exceeding AED 3,500.



South Africa: ALTERNATIVE – **account verification services** are available as opt in services on a per-transaction basis at an extra cost.



Nigeria: ALTERNATIVE – Implemented account resolution where customers select a bank and an account number, and the banking application returns the name of the recipient account as per the beneficiary's bank records. The namecheck is done by the customer at the point of initiation within the banking channel.



Spain: EXPLORATION – Testing and starting to introduce CoP mechanisms.



Italy: EXPLORATION – Testing and starting to introduce CoP mechanisms.



France: EXPLORATION – Testing and starting to introduce CoP mechanisms.



Germany: EXPLORATION – Testing and starting to introduce CoP mechanisms.

How will success stories set the trend for other regions?

In conversation with Finextra, Adrian Smyth, head of domestic payments and innovation, NatWest, states that success has been perceived “in the areas of fraud and error prevention since the introduction of CoP in the UK in 2020. A learning from the initial phase was that fraudsters then targeted customers of those financial institutions who were not yet CoP enabled. Further CoP expansion has helped to address this and we have seen further expansion in late 2024 across 300+ firms as directed by the PSR.” The facts are clear: enabling CoP reduces fraud.

If more quantitative evidence was needed, Nounou adds that “by October 2023 CoP in the UK had achieved 99% of all CHAPS and faster payments, the group 2 deadline for SD17 (Specific Direction 17) was already showing promising results with a 17% reduction in APP fraud in 2023.

“However, compared to initiatives like the IBAN name-check in the Netherlands, which achieved an 81% reduction in fraud within **foreign domestic transfers**, CoP’s impact might seem less impressive. Nonetheless, both these successes serve as a blueprint for other regions aiming to bolster their payment security frameworks,” Nounou says.

Moriarty agrees that the UK and the Netherlands should be examples that we place on the pedestal for other countries and regions to emulate. “The implementation of CoP in the UK has shown positive impacts in reducing accidentally misdirected payments and APP fraud. Data from the PSR has shown that CoP has resulted in customers abandoning potentially fraudulent transactions that they otherwise would have proceeded with.

“Financial institutions utilising CoP have reported that it improves security and boosts customer confidence when making payments to new payees. Data has also shown a reduction in relevant APP scam types at banks with CoP implemented, compared to an increase at banks without it. This success provides a strong rationale for wider adoption across the EMEA region. By proving that a real-time account verification check can significantly deter fraud attempts, the UK experience lays the groundwork for similar systems to be replicated globally. Regions like the EU adopting IBAN verification under PSD3 are taking inspiration from the initial achievements of CoP. As more jurisdictions see the tangible fraud reduction benefits, account verification capabilities are expected to become a standard anti-fraud safeguard adopted internationally in the future,” Moriarty explains.

But what should regions such as APAC and North America consider before legislating CoP? In Mihail Duta's view — director, solution consulting, Finastra — there are three factors, as clarified below:

- **Detailed regulation:** Clear and detailed regulations provide a framework for all stakeholders to understand their responsibilities and the standards they need to meet. This helps in creating a consistent and secure environment for transactions.
- **Single API:** A single API for payment verification services simplifies integration for financial institutions. It allows for a more streamlined process, reducing complexity and the potential for errors, which can be a significant advantage when replicating success in different regions.
- **Strong regulatory framework and governance:** A robust regulatory framework ensures that there is oversight and accountability. Governance structures support the enforcement of rules and the resolution of disputes, which is essential for maintaining trust in the payment system.

These factors should instil confidence in financial institutions and PSPs to improve their payments systems, consider their unique regional challenges, establish a country or continent specific CoP scheme, and join the global race against fraudsters. However, while every country wants to reduce fraud across payments because they want more control over their transactions, this is harder to do with international payments.

As Duta elucidates, domestic CoP is simpler because it “operates within a single country's banking system and regulatory environment. The names and account details are usually standardised and consistent, making the verification process more straightforward.” However, international CoP processes can get lost in translation and multilingual name matching may not suffice. Biometric solutions such as phonetic fingerprint technology may have to play a role.

Nounou explains that “domestic payments are driven by local market infrastructures such as Pay.UK in the UK” and “CoP operates in a peer-to-peer manner, directly validating payment details between the payer and payee within the same country.” International payments pre-verification, on the other hand, “is more complex due to the need for interoperability between different countries' payment systems. The SEPA Inst mandates and the use of a centralised architecture, often facilitated by intermediaries, play a crucial role in the international implementation of VoP. However, enhanced data standards such as ISO 20022 improve the accuracy and efficiency of cross-border fraud checks.”

03

Asia Pacific

What is the state of play for APP fraud and misdirected payment fraud across APAC?

Eli Shoshani, head of APAC, Bottomline, calls upon the industry to consider “the implementation of payment verification mechanisms in APAC. The landscape of payment fraud prevention is marked by significant efforts to enhance verification mechanisms, both for domestic and international transactions.” He goes on to say that two-factor authentication (2FA) is a “standard approach in many APAC countries, involving verification via phone numbers and emails. This method ensures that a transaction is authenticated by a secondary method besides the account credentials.

Alongside this, as Shoshani explains, “in countries like Malaysia, Indonesia, Japan, and Australia, there is a strong emphasis on verifying account numbers against phone numbers and email addresses as part of their faster payment schemes. This verification process is embedded within the national payment schemes rather than being a responsibility of individual banks.” These techniques are used for domestic payments, but for cross-border payment verification, heavy reliance is on Swift to facilitate bank account verification (BAV), sanction screening, behavioural monitoring and leveraging the benefits of enhanced data standards such as ISO20022.

Southeast Asia

Southeast Asia’s digital ecommerce activity may be thriving, but it could be argued that sales growth such as this is linked to an increase in social engineering attacks, such as scams and account takeovers (ATOs). It is evident that as APP fraud becomes more prevalent, fraud solutions that include an account verification feature or CoP will be required.

The UN also released a report estimating that at least 120,000 people in Myanmar and around 100,000 in Cambodia “may be held in situations where they are forced to carry out online scams.” Shedding light on the fact that workers are trapped in virtual slavery, the findings reveal that they themselves

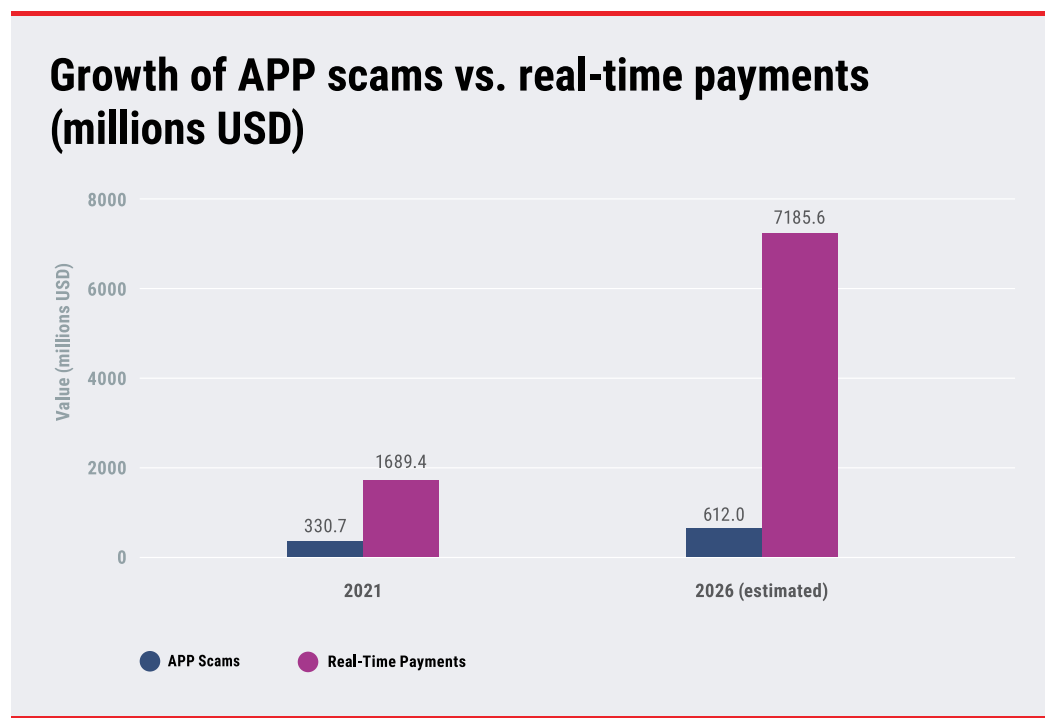
are trapping vulnerable consumers into romance ploys, fake investments and illegal gambling schemes. Laos, the Philippines and Thailand are also among the countries where criminal gangs set up online fraud operations.

A **United States Institute of Peace** report revealed that:

- \$43.8 billion is stolen through scams by criminal groups in Cambodia, Laos and Myanmar each year.
- \$12.5 billion is the estimated return on cyber scamming with many compounds owned by local elites each year.

South Asia

Considering India as an example, ACI Worldwide research found that social engineering has increased by 50% in just four years. The firm refers to this situation as escalating “into a political hot potato, with fever-pitch media coverage fuelled by abundant stories of vulnerable people losing their life savings.” While many of the scams have taken place because of an influx of first-time users of the UPI (Unified Payments Interface) real-time payments system, this is ultimately positive development as digital transformation has led to financial inclusion, but CoP regulation will have to come to the fore to mitigate the sheer number of scams.



Source: ACI Worldwide – an overview of growth of APP scams in comparison to real-time payments in India.

Northeast Asia

Japan has emerged as the world's fourth largest ecommerce market next to China, the United Kingdom, and the United States. However, according to **Forster**, what sets Japan apart from its Asian and Western counterparts is its low to even zero domestic ecommerce fraud rates. Relying on 3DS, fraud tends to be cross border, with fraudsters outside of Japan targeting Japanese consumers.

For instance, APP fraud in Japan is increasing – but for the first time in a while. As reported in **The Japan Times**, 2022 figures “marked the first rise of recognized criminal offenses in 20 years, mainly due to the easing of COVID-19 restrictions. The numbers rose again in 2023, with 703,351 recognized criminal offenses, a 17% leap from 2022. However, NPA officials say that is premature to conclude that the public safety in Japan has deteriorated.”

19,033 cyber and phone scams, an 8.3% increase from 2022, marking the highest level in 15 years, were recorded in 2023.

The Pacific

Mihail Duta, director, solution consulting, Finastra, highlights that “Australian consumers are increasingly moving online, with a significant portion of retail sales turnover taking place online. However, this shift has also led to a rise in data breaches and gift card fraud.” **Australia Post's** 2022 eCommerce Industry Report confirms this and states that while the market will reach up to \$35 billion by 2025, it will be accompanied by an increase in data breaches, causing additional fraudulent activity as criminals access a broader set of data to leverage.

He continues: “The APAC region's approach to combating payment fraud includes leveraging technology and regulatory measures to protect consumers and merchants. As the region is home to more than half the world's population, the strategies and solutions implemented here can have a global impact on the fight against payment fraud.” In the same way that fraud solutions with name checking features can have a global impact on fraud prevention, non CoP initiation can have a negative effect on international payments.

Which countries/regions have implemented CoP within APAC?



India: EXPLORATION – Emerging and will pave the way for CoP in the APAC region, but not yet mainstream.



Singapore: ALTERNATIVE – Implemented BAV and VoP at the domestic level, ensuring pre-validation of payee details before transactions are completed.



Thailand: ALTERNATIVE – Implemented BAV and VoP at the domestic level, ensuring pre-validation of payee details before transactions are completed.



Vietnam: ALTERNATIVE – Implemented BAV and VoP at the domestic level, ensuring pre-validation of payee details before transactions are completed.



Indonesia: ALTERNATIVE – Implemented BAV and VoP at the domestic level, ensuring pre-validation of payee details before transactions are completed.



Malaysia: ALTERNATIVE – Implemented BAV and VoP at the domestic level, ensuring pre-validation of payee details before transactions are completed.



Hong Kong: ALTERNATIVE – Implemented BAV and VoP at the domestic level, ensuring pre-validation of payee details before transactions are completed.



Pakistan: ALTERNATIVE – Implemented account resolution. Using this mechanism, customers select a bank and an account number, and the banking application returns the name of the recipient account as per the beneficiary's bank records. The namecheck is done by the customer at the point of initiation within the banking channel.



Japan: ALTERNATIVE – Implemented account resolution.



Australia: ALTERNATIVE - Uses Swift for both domestic and international BAV, incorporating VoP mechanisms.

Duta summarises that there is no exact match for the UK's CoP or the EU's VoP in the APAC region. "The ability to perform beneficiary name match can be done well in this region, however, where the 'engine' in each country may be different, the result would be close to a VoP/CoP service. Many of these regions can provide coverage of greater than 90%. For example, India, Pakistan, Indonesia, Vietnam, South Korea and China have 95% penetration to retail accounts."

What is the impact of non CoP initiation on international payments?

While alternatives or similar pre-verification schemes to CoP are being implemented in APAC, the guardrails that are required across international payments are missing, and there is not enough legislation to mandate sufficient confirmation of payee when making cross-border payments. In addition to this, when scams occur and money is lost, the emotional variability and the uncertainty involved with being a victim of fraud in an international scenario – although the similar kind of risk – becomes more extreme and aggravated.

Duta agrees and says that "the lack of a standardised payee verification process can indeed lead to delays in payments delivery due to the need for additional checks and investigations. These measures are necessary to prevent fraud but can be time-consuming and costly. Moreover, the return rates for international payments are significant, with a notable percentage attributable to errors in beneficiary information, such as incorrect names or account details. The implementation of CoP/VoP can help reduce these errors by ensuring that the payee's details are verified before the payment is processed, leading to more efficient and secure transactions."

In Shoshani's view, the absence of pre-verification mechanisms like CoP and VoP can have several detrimental effects on the efficiency and security of global payments. They are summarised below:

- **Delays in Payment Processing:** Without pre-verification, payments often face significant delays. This is particularly problematic for international transactions where time-sensitive transfers are crucial.
- **Increased Verification Costs:** Banks incur higher costs when verifying unknown payments manually. This can be a significant financial burden and reduce operational efficiency.
- **Payment Friction and Client Dissatisfaction:** The lack of streamlined verification leads to friction in payment processes. Customers experience delays and increased likelihood of errors, leading to dissatisfaction and potential loss of trust.

- **Missed Payment Deadlines:** Transactions without pre-verification are more likely to miss cut-off times, which can be critical when only limited periods are available for sending transactions. This is especially important in regions where real-time payments are becoming the norm.
- **Limited 24/7 Operation Capability:** Non-adoption of pre-verification initiatives hampers the ability to provide round-the-clock payment services, which is increasingly expected in the global financial landscape.

The APAC region is paving the way for innovative, or at least, functional APP fraud prevention with 2FA and account verification for domestic payments, alongside Swift-facilitated BAV for cross-border transactions. However, the yet to be implementation of CoP and the difference in adoption of VoP across countries highlights that greater standardisation and integration of pre-verification tools is needed. Technology can help address these issues by automating these requirements, which in turn will significantly reduce payment delays, cost, and friction. This will then hopefully enhance client satisfaction and operational efficiency across the global payment ecosystem.

04

North America

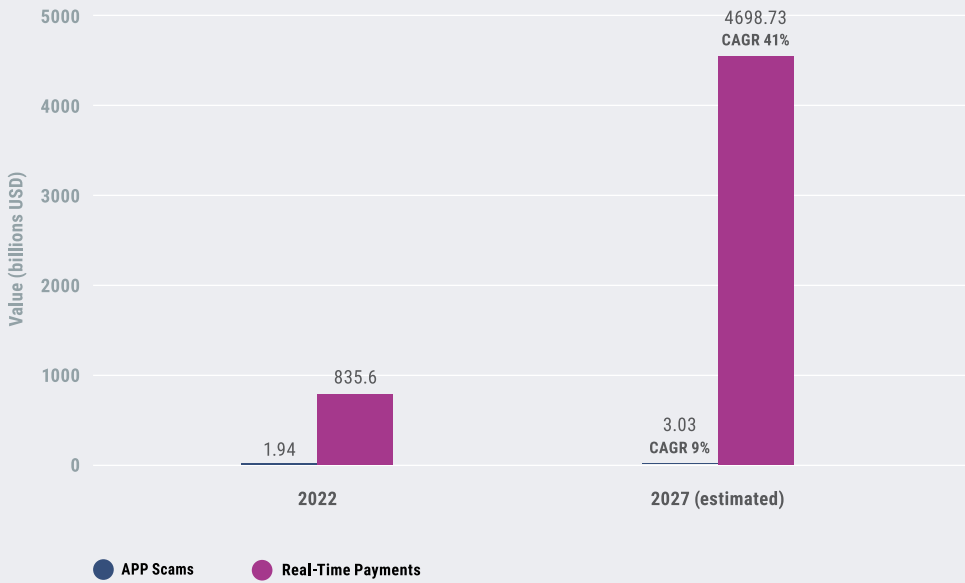
What is the state of play for APP fraud and misdirected payment fraud across NA?

In conversation with Finextra, Mihail Duta, director, solution consulting, Finastra set the scene for domestic and international payment fraud in North America, which he referred to as “a matter of ongoing concern, with fraud costs and key performance indicators (KPIs) increasing for a second consecutive year. Despite this, most merchants have not increased the share of revenue they spend to manage fraud.” The latter point could be an issue; if CoP is not mandated on a country or state level, in the case of the US, it is up to the merchants, PSPs, or financial institutions to ensure they are budgeting for and investing in fraud solutions that provide the level of pre-payment verification that is needed in 2025 and beyond.

United States

With the US Federal Reserve’s real-time payment service FedNow going live in 2023, as with any new payments rail, this will attract a number of fraudsters wanting to take advantage of any vulnerabilities within associated channels. Scammers are likely to continue to use social engineering to encourage users to send money from account to illicit account at the same speed as the real-time payment network is scaled up. In the same way that uptake of India’s UPI payment rail resulted in an increase of APP fraud, as FedNow usage becomes more mainstream, financial institutions and PSPs will need to be conscious of potentially increased, sophisticated, APP fraud. While the Federal Reserve provides fraud identification tools, this is not enough, and organisations must not hesitate before implementing confirmation of payee or liability models. To reiterate, organisations must evolve at the same rate as their competitors and their enemies – the fraudsters, and this may mean prioritising AI adoption to support behavioural profiling and other prevention methods.

Growth of APP scams vs. real-time payments (billions USD)



Source: ACI Worldwide – an overview of the growth of APP scams in comparison to real-time payments in the US.

Canada

Canadian-based fraud significantly outpaced the global rate with a 39% increase in 2023 from 3.6% in 2022. While this number had slowed down to an industry average of 11% growth YoY in scams in the first half of 2024, it is evident that Canada is not prepared for this level of attempted APP fraud. For traditional banks that are currently at risk of disintermediation, this is problematic. Because fraud risk and security concerns have influence over who customers choose to do business with or bank with, and if a particular bank, PSP or merchant does not have the proper pre-payment verification features, users will also be concerned about their personal data being compromised. It is a virtuous circle, but most challenges can be resolved or minimised with CoP.

Transunion data finds that:

- Scam and authorised fraud was the most prevalent fraud type in Canada in the first half of 2024, accounting for 31% of reported **fraud losses**.
- **11% growth** in the rate of suspected digital fraud attempts YoY for transactions originating from Canada in 2024.
- **54% of Canadians** surveyed said they were recently targeted with fraud, of which 7% fell victim.
- Canadian business leaders lost approximately 6% of equivalent revenue – representing **\$78 billion** – over the past year (2023-2024) due to fraud.
- **202% increase** in the volume of suspected digital fraud attempts from Canada between 2019-2023.
- **258% increase** in the rate of suspected digital fraud attempts originating from Canada within telecommunications sector from 2022-2023.

Which countries/regions have implemented CoP/VoP within North America?



Mexico: EXPLORATION - In the lead with non CoP/VoP and with greater than 90% coverage in the country. In Brazil, the service is being done as part of Pix, the instant payment scheme, and in Mexico as part of SPEI instant payment.



US: ALTERNATIVE – The National Automated Clearinghouse Association (NACHA) requires financial institutions to perform account validation for account debits that were initiated via online payment methods.



Canada: EXPLORATION – No industry wide **adoption**, “but several banks, like **RBC Europe Limited and Royal Bank of Canada (Channel Islands) Limited** now offers the CoP name checking service.”

What does the future hold for technology solutions that can in fact detect active or inactive accounts?

Duta summarises that with the rise of e-commerce post 2020, “there has been an increase in related fraud attacks faced by merchants, including identity theft, account takeovers, and phishing scams. Businesses are employing a variety of fraud prevention strategies, such as advanced analytics, machine learning, and multi-factor authentication to combat these threats. The management of payments is also evolving, with a focus on optimising acceptance rates and reducing false declines, which can be as damaging as fraud itself.”

He goes on to say that the “landscape of payment fraud is dynamic, and as digital transactions continue to grow, so does the need for robust fraud prevention measures. The trends and strategies in North America can serve as a benchmark for other regions looking to enhance their payment security infrastructure. We are not seeing the American regulator planning a VoP/CoP service in the country, but instead local initiatives that can provide this service.”

Eric Choltus, director of global product management, CFRM (Cyber Fraud and Risk Management), Bottomline, adds that the “fractious nature of payment systems in North America presents a unique challenge when it comes to payment fraud prevention and the implementation of tools like payee verification. Today, there is a growing number of fraud incidents that can be successfully tied back to key trends such as ATO and BEC (business email compromise), but there is no one-size-fits-all approach to solving this for financial institutions and effective strategies often involve the institutions’ ability to leverage various third-party vendors into a cohesive fraud prevention and payee verification strategy.”

Choltus believes that while the way forward is to partner with the technology vendors that can provide efficient and effective CoP or VoP tools, data remains an issue. He says that “datasets are fractured and specialised, and there is minimal national/regional implementation of CoP/VoP in North America.”

However, like a few countries in other regions, account validation and account resolution features are being used and, in the absence of CoP, are a step in the right direction. In the US for example, NACHA requires companies to perform account validation for account debits that were initiated via online payment methods. Choltus adds that “while this is a useful tool for reducing misdirected payments, it is often implemented via a prenote process which can be manipulated by advanced fraudsters. Additionally, there are private payment networks, such as Paymode-X or TCH RTP (real-time payment), that perform payee/payor validations of all network participants prior to allowing them to process funds.”

Partnering with technology vendors can also help to detect active or inactive accounts and minimise false positive alerts links to transaction to new beneficiaries. Choltus goes on to say that to allow “bank investigators to focus on only the most suspicious of these transactions,” defence layers need to be built up with technology to automate some fraud prevention features. They are summarised below:

- **Advanced identity analytics** (IP address, device fingerprint, proxy/VPN detection, etc)
- **Monitoring of online banking session activity** (e.g. beneficiary updates)
- The ability to **correlate fraud analytics** across user login, session activity and monetary transactions
- The ability for fraud investigators to **replay user online banking activity**
- Machine learning for **advanced anomaly detection**
- **Advanced Payee analysis**, including payment history by any bank customer, and payee verification using one or more of the available payee verification tools in the market

Conclusion

Software solutions can alleviate the risk of fraud where CoP is not mandatory. When working with a provider, financial institutions can leverage machine learning to analyse data patterns and identify potential fraudulent activity across a number of industries. With real-time transaction monitoring, device intelligence, data aggregation, customisation rules engines, and as mentioned, machine learning algorithms, fraud can be mitigated but the implementation of CoP is the preferred method of action.

Eric Choltus, director of global product management, CFRM (Cyber Fraud and Risk Management), Bottomline, highlights that the key to fraud detection in commercial banking is “to ensure that bank fraud systems 1) are deeply integrated with the login and online banking/treasury systems, 2) are monitoring and correlating activity across login, session, and payment activity of a customer, 3) have ability to stop transactions in real-time pending investigation, and 4) have the ability to augment analytics with external intelligence.”

Moreover, with APP fraud showing no signs of slowing down, it is evident that legislation mandating CoP on a national or regional basis must be established across the globe. Further, if regulations are not put in place, financial institutions and PSPs must ensure they are leveraging technology solutions to bolster verification mechanisms themselves.

This must be conducted in a way that protects the end customers, adds minimal friction to processes, and assesses current fraud prevention procedures. While success stories in EMEA have set the trend, more needs to be done within the region, and wider adoption is needed in APAC and North America.

About

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology news and information source. It offers more than 130,000 fintech news, features and TV content items to some 800,000 monthly visitors to finextra.com.

Finextra covers all aspects of financial technology innovation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide. Finextra's unique member community consists of over 40,000 fintech professionals and 200,000 social followers working inside banks and financial institutions, specialist fintechs, consulting organisations and technology providers. The Finextra community actively participates in contributing opinions, ideas and comments on the evolution of fintech.

For more information:

Visit www.finextra.com and become a member, follow [@finextra](https://twitter.com/finextra) or reach us via contact@finextra.com.

LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers.

For more information, please visit www.risk.lexisnexis.com and www.relx.com.



Finextra

A Finextra Research report in association
with LexisNexis® Risk Solutions.

Finextra Research Ltd

77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

Telephone

+44 (0)20 3100 3670

Email

contact@finextra.com

Web

www.finextra.com

All rights reserved.

No part of this publication may be reproduced
or transmitted in any form or by any
means, electronic or mechanical, including
photocopy, recording or any information
storage and retrieval system, without prior
permission in writing from the publisher.

LexisNexis® and the Knowledge Burst logo
are registered trademarks of RELX Inc.

© Finextra Research Ltd 2025