Uniting against account-to-account fraud

Lessons from real-time markets

WHITEPAPER
MARCH 2025

Contents

3 Foreword

4 Introduction

5 The complex challenge of fighting fraud in real time

10 Regulation and initiatives: The world looks to leading markets

12 Fighting back against the fraudsters

16 The latest weapons in the fight

19 Conclusion: Boosting trust and resilience

21 How Mastercard is helping in the fight against fraud

Foreword

Johan Gerber
EVP, Security and
Cyber Innovation

Peter Reynolds
EVP, Real Time Payments

Whether it's a romance scammer cajoling a victim to send money to cover "medical bills," or an email from the "CEO" asking the finance team to make an urgent payment, chances are we've all heard of the inventive ways fraudsters are now trying to dupe their victims.

Fraudsters have developed increasingly sophisticated tactics to elicit funds, and then exploited the increasing number of real-time payment (RTP) networks to move and hide this stolen money. With these transactions immediate and irreversible, fraudsters can transfer funds between banks in a matter of minutes, making it almost impossible to trace.

While fraud continues to plague the financial services industry, with the world's consumers losing US$1.03 trillion to scammers in 2024 alone,[1] the fight back is also gathering momentum.

The long-term fight against fraud requires prevention rather than cure. Fraudsters will not simply stop, so we need robust measures that derail fraud before it happens.

At Mastercard, we're committed to doing all we can to win the battle against financial crime. This includes rolling out multi-channel initiatives focusing on both technology solutions and industry collaborations to tackle the problem, as well as working with other bodies to elevate the global awareness of scams and empower consumers and businesses worldwide with the knowledge and tools to protect them from damaging scams.

Introduction

Asim Rai
Manager, Industry Standards
asim.rai@mastercard.com

Alan Baughan
Director, Product Commercialisation
alan.baughan@mastercard.com

Seamless, near instant payments are a hallmark of modern society with RTP systems growing rapidly in recent decades, transforming the way millions of people and businesses around the world transact.

However, as quickly as these near instant payments have taken off, so too has the corresponding risk of financial fraud. In the UK, in 2008 – the year RTPs were introduced – there was a 132% increase in online banking fraud.[2]

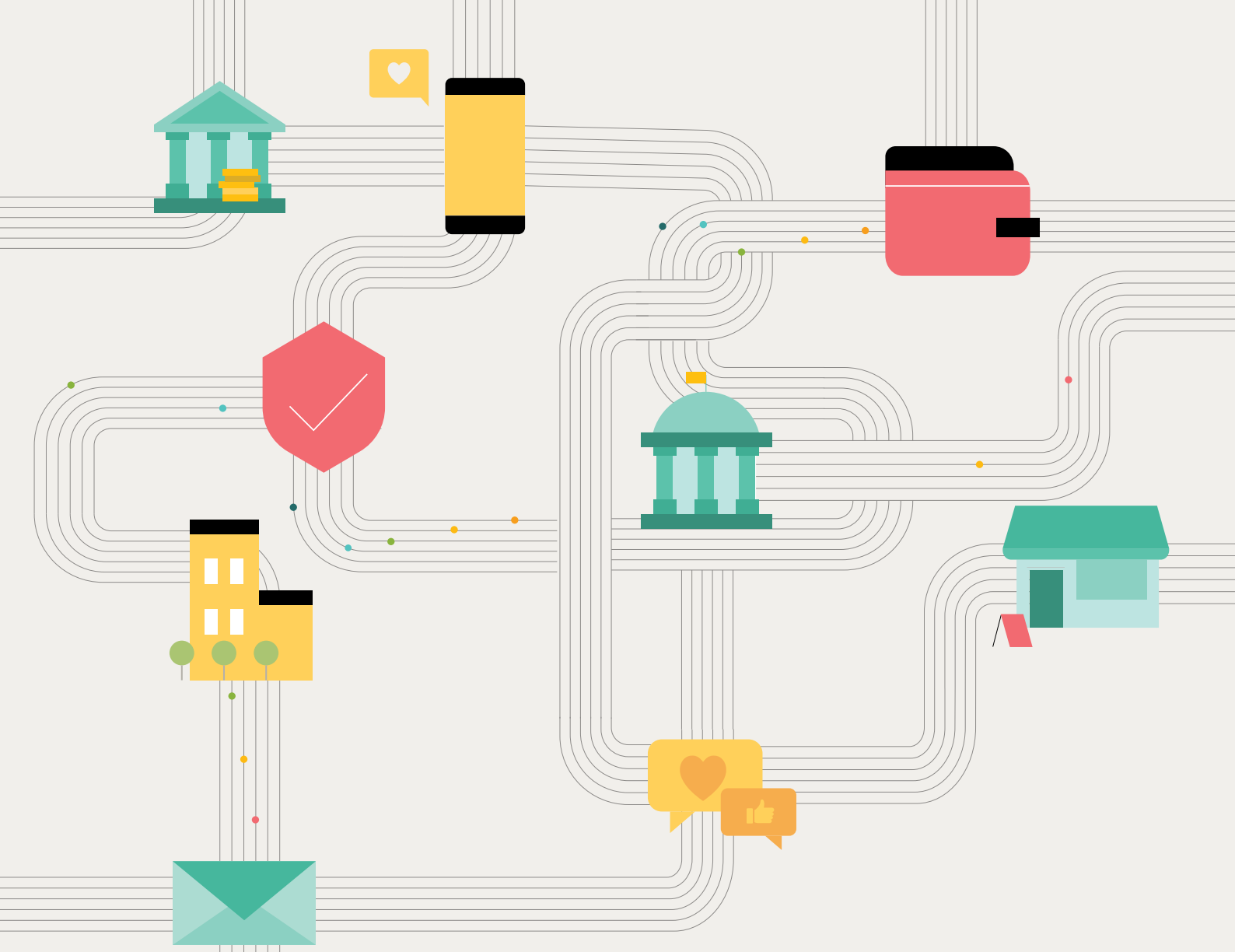
To fight this rising tide requires a collaborative approach across governments, regulators, financial institutions, telecommunications providers (telcos), and big techs including social media platforms. Put simply, fighting fraud must be a team effort.

Governments and regulators in particular have a critical role in ensuring synergy across the ecosystem. In the UK, for example, a new reimbursement regime came into force in October 2024, mandating that financial institutions must reimburse victims of unauthorized push payment (APP) scams when using Faster Payments. The reimbursement is split 50:50 between sending and receiving institutions.

This places greater emphasis on the financial institutions to put in place robust real-time solutions. Technology companies – including Mastercard – are developing data and Artificial Intelligence (AI)-led solutions that banks can embed into their payment systems to identify fraud before it even takes place. However, real-time solutions installed by financial institutions, at the point the transaction is made, only provides a defense against a portion of the end-to-end fraud lifecycle. Protection needs to occur at all stages of the scam lifecycle, both protecting the account at the time the transaction is made, but also the ecosystem. As we'll explore later, Mastercard's unique and comprehensive suite of AI-powered solutions can identify and prevent scams at all stages of its lifecycle i.e. from when a user opens an account, logs in, or makes account changes, to when they carry out transactions.

But with countries around the world at different stages of their RTP journey, and facing different fraud challenges, at present the tactics being implemented to address fraud vary. A better understanding of the strategies and technologies being used in other markets can help pave the way for safer and more resilient services across the global financial ecosystem as new RTP systems are rolled out.

This paper explores these solutions and strategies, offering insights and recommendations to stakeholders across industries as they work together to safeguard the integrity of RTP systems and protect consumers and businesses from fraudulent actors.



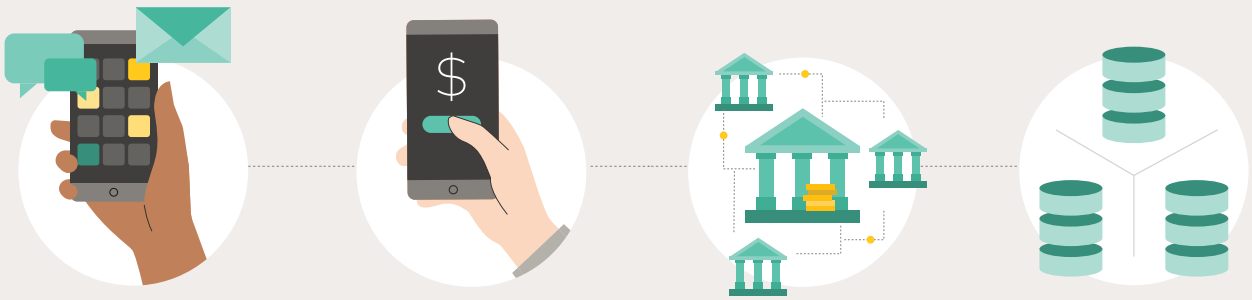
The complex challenge of fighting fraud in real time

There are around 96 RTP systems currently operational across the world,[3] and more markets are planning to implement new systems to boost economies.

The instant nature of RTP systems means transactions are completed within seconds and as a result pose unique challenges when combating fraud. Unlike other payment types, which can be recalled, real-time payments cannot be reversed once processed. The fact that payees can withdraw or transfer funds almost immediately after receiving them makes this type of fraud particularly difficult to detect, stop, and trace.[4]

The impact is felt not only by the individuals who fall victim to this criminal activity, but globally, with far-reaching economic implications.

Traditional fraud detection methods are struggling to respond to modern forms of RTP scams, due to challenges around:



Social manipulation

Where consumers are being coerced into believing fraudulent actors are in fact legitimate agencies.

Customer authorization

Where individuals are willingly transferring often large amounts to illicit accounts.

Rapid dispersal

When RTP systems enable near-instant and irrevocable transactions to be made and dispersed through illicit accounts, making them almost impossible to track and reclaim.

Siloed data

Where various actors involved in the fraud journey hold information about the defrauded consumers and criminals but are currently not sharing as part of the wider picture.

In recognition of these challenges, the first Global Fraud Summit was hosted in London in March 2024, with representatives from the G7, Five Eyes, Singapore, and South Korea agreeing greater collaboration was needed across government, enforcement agencies, banks, and other financial institutions to tackle growing financial crime.

The outcome of this summit was agreement in several key areas, including:

- building international understanding of fraud and partnerships to combat it
- strengthening support for victims, including getting their money back
- better intel and data sharing to aid the pursuit of organized fraudsters
- better government and industry engagement to prevent fraud at its source.[5]

APP fraud presents a unique set of challenges to banks and other entities, including telcos and social media platforms

Types of fraud infiltrating RTP networks

The rise of RTP networks has led to the emergence of specific types of fraudulent activity, which looks to take advantage of the near-instant, irrevocable nature of the transactions it has enabled. This includes:

Micro-structuring – this involves criminals laundering illicit funds by splitting large payments into multiple smaller transfers and often moving them on to separate accounts. Doing this makes it harder for banks and financial institutions to identify these amounts as potentially fraudulent, though a potential indicator could entail frequent incoming and outgoing payments in volumes or amounts that are unusual when compared to similar customers.

Mule accounts – criminals have also taken to utilizing a network of accounts across different individuals. Often referred to as 'money mules', they help criminals to disguise their identity, while making it harder to identify the true origin of the funds.

Identity theft – criminals steal a user's identity, potentially through data breaches, malware or phishing scams, using their financial details to pay for goods and services on e-commerce platforms, or to transfer funds to other accounts via online payment systems.

Authorized Push Payment (APP) Fraud – also known as Authorized Account-to-Account Fraud. This type of scam involves an individual being tricked into transferring funds out of their account to a fraudster.

While all these forms of fraud pose a significant threat to financial institutions and their customers, the rise in authorized account-to-account fraud presents a unique set of challenges to banks and other entities, including telcos and social media platforms as their services are often used by fraudsters for initiating potential victims of authorized account-to-account fraud.

The growing reach of APP Fraud

APP fraud is becoming an increasingly evolving and sophisticated threat. The tools at the disposal of fraudsters are so advanced that even the most technology-savvy victims can be caught out. For example, fraudsters are able to produce deepfake videos with celebrity endorsement that appear genuine, and perhaps most worryingly, AI-powered technology can simulate a loved one's voice to scam victims via a telephone call.

As the adoption and volumes of real-time payments grow, so does APP fraud. Based on reports available, countries like the UK, US, India, Brazil, Netherlands and Australia see some of the highest rates of authorized account-to-account fraud.

United Kingdom

The membership body for UK banks, UK Finance, shows that £460 million was lost to APP fraud in 2023.

A significant portion, 77%, of APP fraud cases in the UK originate from online sources, primarily involving lower-value scams like purchase scams, which accounted for 32% of total losses. In contrast, 17% of cases originated in telecommunications, involving higher-value scams like impersonation fraud, which accounted for 45% of total losses.[6]

United States

Federal Trade Commission (FTC) data shows that U.S. consumers reported losing more than $12.5 billion to fraud in 2024, a 25% increase over 2023, marking the first time that fraud losses have reached that benchmark. Consumers reported losing more money to investment scams—more than $5.7 billion—than any other category in 2024. The second highest reported loss amount came from imposter scams, with losses of nearly $2.95 billion reported.

The Commission monitors trends carefully, and is taking a comprehensive approach to detect, halt, and deter consumer fraud, including leading the largest-ever crackdown on illegal telemarketing. The FTC joined more than 100 federal and state law enforcement partners nationwide, including the attorneys general from all 50 states and the District of Columbia in Operation Stop Scam Calls, a crackdown on illegal telemarketing calls involving more than 180 actions targeting operations responsible for billions of calls to U.S. consumers.[7]

Brazil

The implementation of RTP systems in Brazil (PIX) now has over 165 million individual users.[8] In 2022, it accounted for more than 30% of all transactions, and in turn resulted in an estimated $246.7 million being lost to APP fraud. The majority (74%) of this related to customers making transfers in relation to product, service, or investment. This loss is expected to grow, reaching $635.6 million by 2027.

Many out of the more than 800 financial institutions that participate in PIX are smaller firms with limited Know your Customer (KYC) processes and fraud detection tools that in turn could be contributing to the increase in APP fraud. In this market, criminals are also resorting to extreme tactics like kidnapping in order to force people to authorize payments to mule accounts.[9]

The Netherlands

While the Netherlands has seen a decrease in the damage caused by phishing and other forms of fraud, there was a steep increase in APP fraud, rising to €47.6 million – over 76% of the total €62.5 million reported as the damage caused by all forms of fraud in 2022.[10]

The decrease in phishing fraud is due to anti phishing measures, including consumer awareness campaigns. However, the fact that APP involves coercing the victim makes it more challenging to prevent. We have seen bank-led solutions to this challenge such as ING introducing "check the conversation" functionality on its app which allows Dutch customers to immediately check whether a caller who contacts them is actually an ING employee.[11] This is a great example of a bank fighting back, but fraudsters will always stay one step ahead without wider cross-market collaboration and solutions, something that will be explored later in the publication.

Australia

In Australia, the latest Targeting Scams report reveals Australians lost $2.03 billion to scams in 2024, out of which just under $1 billion was lost to investment scams, with government, law enforcement agencies, and the private sector now looking to improve collaborative efforts to support the community in the fight against scams.[12]

In response, the National Anti Scam Centre (NASC) created a fusion cell dedicated to investment scams, with several recommendations having been made on how to disrupt advertisements, websites, and phone numbers associated with investment scams. Mastercard are part of the NASC and a member of the inaugural fusion cell on investment scams. But the most crucial development is the growing partnerships with law enforcement – primarily the relationships with the NASC and Joint Policing Cyber Crime Centre and Australian Securities & Investments Commission – which has created a regular exchange of scam intelligence to inform enforcement prioritization by relevant law enforcement agencies.[13] Furthermore, financial institutions have united to create Safe Scam Accord – a proactive initiative to install a wide-ranging set of anti-scam prevention measures across the entire industry.

Regulation and initiatives: The world looks to leading markets

Given APP fraud relies on someone authorizing the movement of funds to a fraudster's account, individuals have often been deemed fully responsible with no recourse for reimbursement from their financial provider.

However, with the scale of APP fraud unabating, there are growing calls to establish clearer lines of liability for this across financial providers, social media platforms, and telcos.

In the UK, for example, the Financial Conduct Authority (FCA) has urged financial services firms, as well as other businesses like social media platforms, to do much more in combating financial crime.[14] As a market with one of the most mature RTP systems (as well as high cases of APP fraud), the world is closely watching the UK to understand how to safeguard best against the spread of financial fraud.

The UK moves towards joint liability

In 2023, the UK Payment Systems Regulator (PSR) announced new measures to further protect consumers against APP fraud, with the introduction of a new mandatory requirement for all UK financial providers to reimburse customers who fall victim to APP scams in all but exceptional circumstances.[15] Having come into force in October 2024, the new framework stipulates reimbursement costs will now be shared between the sending and receiving financial providers (so both the customer's financial provider and the provider used by the fraudster).[16]

Some in the industry have critiqued the approach of focusing only on financial institutions, with Innovate Finance, an industry body representing the UK's fintech community, critical of making banks and other financial providers 'solely liable' for reimbursement when an estimated 60% of all APP fraud originates on social media platforms.[17] Some payments firms had called for a rethink, arguing that a refund cap of £415,000 will hurt fintechs and smaller providers – and therefore competition.[18]

Consistent minimum standards offer customers greater protection but will also pose several challenges for financial institutions. Not only will they need to adapt to these changes before the end of 2024, but the shift to joint liability between sending and receiving entities and a high maximum level of compensation will necessitate increased levels of collaboration between institutions.

Singapore goes phishing with the telcos

Another mature RTP market featuring high levels of fraud is Singapore, which was hit by 32 million digital fraud attacks in 2022 alone.[19] While online sources are the main point of origination for fraud in many other markets, telecommunications is the major origination point in Singapore.

In 2022, for example, OCBC Bank customers were hit by a sophisticated SMS scam, costing a total of S$13.7 million. This led to a subsequent agreement to make goodwill payments to all those affected.[20] In response to such incidents, Singapore's government has drafted the Shared Responsibility Framework (SRF) to confront the growing prevalence of fraud in digital payments.

Led by the Monetary Authority of Singapore (MAS), the SFR seeks to mitigate losses stemming from phishing scams and spread accountability for losses amongst financial institutions, payment service providers, and telcos.

For banks, the framework outlines new responsibilities, including implementing a 12-hour cooling-off period if required during which 'high risk' activities cannot be performed; providing real-time notifications for high-risk activities; issuing outgoing transaction alerts in real time; and offering a 24/7 reporting channel for consumers to immediately block their accounts to prevent further unauthorized transactions.

Telcos are also expected to increase their responsibilities in these areas, including ensuring these messages only originate from legitimate registered senders; blocking SMS messages from unauthorized aggregators (organizations that collect large volumes of texts from brands and distribute to wireless carriers) to prevent the delivery of messages originating from unauthorized networks; and implementing an anti-scam filter across all SMS to block messages containing known phishing links.

MPs in Singapore responded to the framework in early 2024, saying it was a step in the right direction, but emphasized more needs to be done to enhance customer protections, namely because the measures do not ensure reimbursement for victims of fraud.[21]

Fighting back against the fraudsters

To tackle the account-to-account fraud issue, we need to embrace a multi-channel approach that includes both technology solutions and industry collaborations. In addition, we need to elevate the global awareness of this type of fraud, set new industry standards, and empower consumers worldwide with essential anti-fraud education.

To truly combat fraud, industry collaboration is essential

As has been seen from the examples of Singapore and the UK, entities involved in the fraud journey (including financial institutions and telcos) are coming under increased pressure to put in place firmer protections and processes to halt illicit activity before it has even taken place.

Yet effective progress in this area will rely on collaboration across banks and other financial providers, regulators, governments, telcos, big tech and social media platforms going further.

"We need to bring together data and insights from all entities involved in the fraud journey."

A telco, for example, may have insight into the behavior of a smartphone user that is not visible to a financial institution, which in turn could be used to help detect fraudulent activity. This might include whether the user has interacted with a recognized fraudster's mobile number or is on a call at the same time as a financial transaction is taking place (an often-telltale sign of coercion).

Fraudsters are already working across the entire range of platforms and services in order to convince victims to willingly transfer funds out of their accounts. As such, solutions to combat this must also look to bring together data and insights from all entities involved in the fraud journey.

Greater collaboration across sectors and industries, with governments and regulators spearheading this action, will be crucial to ensuring the full range of data and insights from financial institutions, telcos and social media platforms can be brought together to develop the tools and solutions needed to identify and intercept fraud. But there are a number of actions financial institutions can take now to get ahead and lay the groundwork for greater collaboration.

52%

of consumers more likely to open accounts digitally than they were a year ago

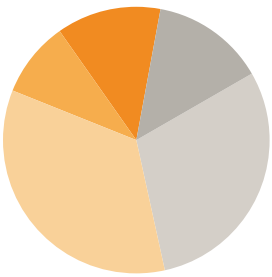
The optimal way to stop APP fraud, or any fraud type for that matter, is to prevent fraudsters from opening bank accounts in the first place

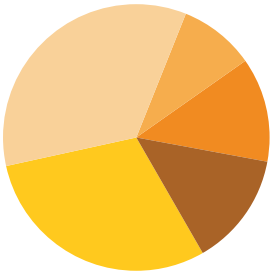
When customers are opening accounts, Know Your Customer (KYC) processes are designed to prevent fraudsters from stealing identities to create fake accounts from which to send and receive stolen funds. But with 52% of consumers more likely to open accounts digitally than they were a year ago,[22] identity verification is becoming more complex for financial institutions and the people that use them.

The problem is that synthetic identity theft – when a fraudster creates a false identity by combining real and fake information – is often missed in traditional KYC processes because each individual identity element is real – it's only the way they're linked together that uncovers their fraudulent nature. This again underlines the importance of breaking down data silos to allow financial institutions to build a more holistic picture of potential customers.

Despite enhanced KYC checks, fraudsters will continue to find ways to access bank accounts – whether their own, fraudulent ones, or via 'money mules' – and given the speed and irrevocability of RTP systems, real-time monitoring of payment flows is needed to safeguard customers.

"The full benefits will only be realized when all participants adopt the ISO 20022 standard."





Data is king

In years past, when financial institutions actioned a transaction, it was just the funds that were processed and sent. But one major transformation we have seen in recent years is the ability for financial institutions, when processing a transaction, to send crucial data along with those funds.

The transfer of richer and structured data along with financial transactions can enable the swift identification of fraudulent activity. The industry's adoption of a global standardized messaging in the form of ISO 20022 has the ability for this data to be passed end to end, from bank to bank and country to country, allowing the multiple parties involved in investigating and resolving fraud cases to work more collaboratively. The additional data points within the messages such as the payment purpose codes and structured remittance information allows for more granular analysis of transactions helping financial institutions identify unusual patterns or anomalies that might indicate fraud. These data points can be further utilized to understand customer behavior and risk profile over time.

Additional transaction data can also help reduce the number of false positives generated by fraud detection systems by providing more context and detail about transactions. This will allow institutions to focus their resources on investigating genuine threats and improve the overall effectiveness of their fraud prevention efforts, but the full benefits will only be realized when all participants adopt the standard.

One example of collaboration in this area is between India and UAE where they have introduced Purpose Codes, which are four-letter codes that indicate the reason behind a payment. Consistent use of these codes allows banks and other financial institutions to identify potentially fraudulent transactions. For example, high value payments from retail customers marked with 'business expense' might raise a red flag.

"Fraud costs financial institutions over four times the amount defrauded."

Getting on the front foot

While governments and regulators across the globe are taking steps to increase collaboration and set expectations on industries in the fight against fraud, many financial institutions are already taking steps to enhance their procedures and systems in this respect.

The risk for financial institutions that wait for regulators to act, and then react to close specific gaps, is that it could prove costlier than proactively implementing something earlier on that aligns with a bank's broader risk management strategy.

Acting early to combat fraud can not only ensure banks and financial institutions get ahead of potential regulatory requirements, but also has wider benefits in terms of customer retention and reputation. For example, a survey among PIX users in Brazil who had been victims of fraud found that 37% had changed their banks after the incident, while 31% stated that their level of trust in the financial institution decreased afterwards.

In the UK, inbound payments monitoring has arguably become the single biggest priority for all financial institutions because of the liability shift. Many don't have the full suite of mitigation tactics required, other than traditional Mule detection, which isn't sufficient in identifying inbound fraud. This is a net new area for most financial institutions and could prove very costly if they do nothing.

To complicate matters, the cost of fraud to a financial institution far outweighs the costs of the financial crime itself. A 2023 Lexis Nexis study in North America found that fraud costs financial institutions over four times the amount defrauded as the cost not only includes the value of the fraudulent transaction itself, but also the fees and interest incurred during the applications, underwriting and processing stages, fines and legal fees, as well as costs in investigating and recovering any expenses.[23]

Getting on the front foot is clearly in the interest of financial institutions, enabling them to put in place systems and procedures that complement existing strategies, rather than being compelled to take action in a certain way by external actors.

The latest weapons in the fight

Inbound and outbound transaction monitoring

UK banks have been among the first in the world to utilize network-wide outbound transaction monitoring solutions that intercept and halt potentially fraudulent activity (with inbound monitoring planned to launch later in the year). Thousands of identity, behavioral and transactional data points are fed into models that provide risk assessments to verify a valid transaction or flag the probability of a scam. The tool doesn't just focus on identifying the recipient as a potential fraudster, but it also detects if the sender is transacting out of pattern.

While these solutions alone aren't a silver bullet, they enable banks to overlay the findings with their existing fraud controls, including transaction monitoring solutions or fraud risk management platforms, and can significantly enhance their arsenal in the fight against fraud.

Anti-fraud engine and alerts

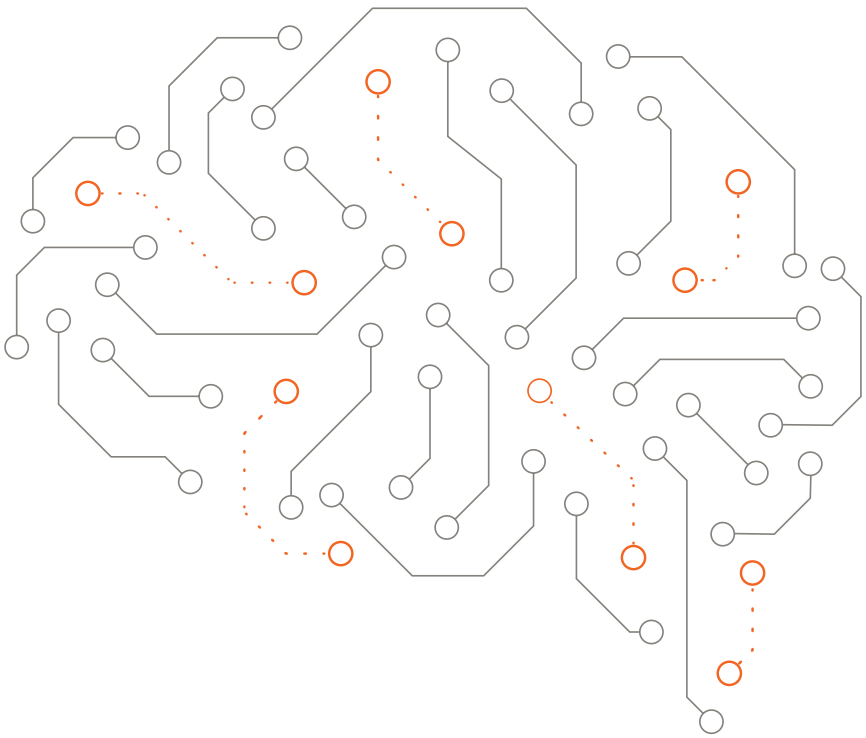
The Faster Payment System (FPS) Suspicious Proxy ID Alert was launched by the Hong Kong Monetary Authority (HKMA) in November 2023. HKMA is collaborating closely with the Hong Kong Police Force (HKPF) and the financial services sector to develop an alert mechanism based on information available from Scameter, an anti-fraud engine developed by the HKPF.

Users will be alerted if a payee's FPS proxy ID (such as mobile phone number or email address) falls within the list of proxy IDs labeled as 'high risk'. An alert will then be displayed to the user, prompting them to think twice before deciding whether to cancel the transaction or continue with the payment.

Confirmation of Payee

Confirmation of Payee (CoP) allows consumers and businesses to verify the recipient account's name and match it to account number and sort code before making a payment. If discrepancies are detected, CoP alerts users to potential risks.

In the UK, the PSR has also noted its effectiveness in reducing misdirected payments since its introduction by the big six banks.[24]



Enhanced data and machine learning

With more data to draw on, such as historic transactions and customer behavior patterns, machine learning algorithms will be able to better analyze this data to identify patterns and anomalies, informing financial institutions of the risk of fraud.

While already being used by financial institutions, further utilizing Artificial Intelligence (AI) and machine learning (ML) will only become more essential in combating financial crime and fraud. The ability to use these tools to establish patterns and profiles, predict behavior and detect anomalies are the core strengths of AI and ML technologies. They also provide a good foundation on which to build a comprehensive solution for fighting fraud and reducing risks.

The next step for data and machine learning is to build an even clearer picture of the person sending and receiving the funds using data from other sources often involved in the fraud journey, such as telcos and social media platforms. Governments and regulators have an important role here as a convenor, bringing these different actors together in greater collaboration, both voluntarily and through legislation. Initiatives like the Global Fraud Summit in London in March 2024, which shows how the UK is taking a leading role in responding to the threat of APP fraud, are essential to facilitating this ongoing discourse.

Next generation solutions

The next generation of solutions must be designed to complement efforts by individual banks which would otherwise be confined to their own networks.

This is because banks can only see within their own 'four walls'. They can only see the transactions that occur within their systems and therefore can only train their models on their own historical data. Finding new ways to allow financial institutions to securely share data via a consortium model will help providers to accurately analyze money flows and use predictive intelligence to identify fraud and prevent crime before it can take place. Crucially, this can all take place without compromising the speed and certainty that consumers have come to expect from RTP systems.

Importantly, the new wave of solutions must be able to also span the various touchpoints in the scam lifecycle, including account opening, login, modification, and recipient addition/modification. Each touchpoint should be accompanied by specific capabilities aimed at preventing scams, leveraging data across personal, behavioral, and device parameters.

Conclusion: Boosting trust and resilience

RTP systems have revolutionized the way we conduct financial transactions, offering unprecedented speed and convenience. However, this improved user experience comes with an escalated risk of fraud and financial crime, particularly with the rise of APP scams.

In this paper, we shed light on the increasing prevalence of APP scams, highlighting the existing work that is already stemming the tide, but also the urgent need to enhance coordinated efforts to combat fraud.

To succeed in the long run and to protect people from scams we need a multi-layered approach:

- **New technologies hold the key.** New technologies being developed by providers are the next step in enhancing security and mitigating fraud risks. Only by utilizing advanced data analytics and machine learning capabilities, and through widespread adoption of these tools, can we hope to enable swift identification and prevention of fraudulent transactions.

"Together we can boost trust, security and resilience in real time financial transactions."

- **Enhanced data sharing.** Machine learning tools are only as effective as the data they are built on. With collaborative efforts to share data from across financial institutions – following the consortium model being explored in the UK – providers will have greater access to the information needed to create effective solutions to identify and stop fraud before it occurs

- **Cross-sector collaboration.** The fraud 'journey' starts way before the transaction, so it is critical for banks and other financial institutions to work with telcos, social media companies, and other parts of the ecosystem to bake in appropriate controls. Banks need a wider view across the customer, their behavior, and their device to collectively use these insights to protect against scams. Regulation can help to ensure a consolidated approach, but it will need to straddle multiple industries, and this is where governments could step in, rethinking the application of current laws which can often restrict data sharing, such as GDPR in the European Union and the Bank Secrecy Act (BSA) in the USA.

- **Proactive not reactive.** Rather than waiting for new requirements to come into force, financial institutions should be anticipating these changes and striving to keep ahead of the regulatory curve. This might include adopting the new technologies outlined in this paper or working with industry bodies to drive sector-wide initiatives.

By adopting a proactive and multi-faceted approach to fraud prevention, we can together boost trust, security, and resilience in real time financial transactions, ultimately ensuring a safer and more secure financial ecosystem fit for the digital era.

How Mastercard is helping in the fight against fraud

Mastercard announced Scam Protect in April 2024, a suite of specialized solutions powered by cutting-edge AI technologies. It is focused on identifying and preventing fraud across the scam lifecycle, from when a user opens an account, logs in, or makes account changes, to when they carry out transactions.

Scam Protect is built on three key pillars that include:

Technology solutions

Our advanced AI-powered Identity insights examine digital footprints and assess unique patterns to detect risk and flag suspicious activity indicative of scams.

Industry collaboration

We collaborate across industries, partners and organizations worldwide to secure the digital ecosystem, ensuring payments are safe for all. Combating the growing threat of scams demands a collective effort.

Market education

We work with and through our collaborators to provide knowledge and tools that help people protect themselves and their loved ones from scams, while also working to destigmatize the experience of being a victim.

Data-led solutions

We are working closely with stakeholders from across the industry to help them prepare for shifting liabilities and, developing the data-led tools that can be utilized by a financial institution to notify them of potential high risk transactions.

Mastercard's tools can be utilized by both sending and recipient financial institutions. It can identify and halt potentially fraudulent transactions in real-time, while notifications shared with transactions to receiving institutions can enable them to act if they suspect illicit activity. This helps both the sending and receiving institutions to work together, making it harder for criminals to bypass security procedures.

How inbound transaction monitoring works

- A consumer unknowingly attempts to send funds to a scammer
- Mastercard leverages AI, machine learning and data points built on billions of transactions which feed into multiple algorithms and models
- Mastercard analyzes network, relationship and transation risk markers to provide a consolidated near real-time risk score in milliseconds
- This pre-transaction risk score enables banks to identify high risk transactions and stop funds before they leave the consumer's account

APP fraud performance data shows that banks in the UK with the lowest fraud rates are using Mastercard's inbound transaction monitoring tool.[25] TSB, for example, found that in just four months, it had dramatically increased its fraud detection rates. Based on TSB's results, the amount of scam payments prevented over a year would equate to almost £100 million[26] saved across the UK, should its performance be mirrored by all banks.

Continuous learning

With the evolving nature of financial crime, Mastercard's reach across markets, entities, and sectors is a powerful means of combating the spread of fraud, with real-time analysis of billions of data points and the detection of suspicious activity across all money movement flows. Having access to all this data allows us to create a continuous learning feedback loop, trained by machine learning, which means financial institutions stay on the front foot when combating fraud. The financial institutions that aren't proactive in this area will become the chief targets for fraudsters.

Educating consumers

While collaboration between entities involved in the fraud journey is crucial, helping consumers to understand the tell-tale signs of fraud is also critical.

That's why Mastercard is a supporting member of the Global Anti-Scam Alliance, and we advocate sharing knowledge and defining joint actions to drive safer and more secure ways to transact, interact, and protect consumers.

As part of the Alliance, we recently helped establish a chapter in Singapore, bringing together organizations in the region to work on rolling out new solutions. Mastercard will continue to partner with organizations like the Global Anti-Scam Alliance that are helping to build new security standards that will protect people and businesses around the world.

Footnotes

1. Global State of Scams Report 2024.
2. The Rise of Fraud Threats and the Implications of Canadian Payments Modernization: How Soon is Now? (Actimize Ltd., 2020).
3. The Real-Time Payments World Map (PYMNTS.com).
4. Federal Reserve, Fraud and instant payments: The basics.
5. Gov.uk.
6. UK Finance.
7. Federal Trade Commission.
8. PCMI.
9. Scamscope Report: APP Scam Trends (ACI Worldwide).
10. Nederlandse Vereniging van Banken.
11. ING.
12. Targeting scams: report of the National Anti-Scam Centre on scams data and activity 2024.
13. Investment scam fusion cell, Final report (ACCC).
14. FCA calls on firms to be bolder in the fight against financial crime (pinsentmasons.com).
15. Lending Standards Board.
16. Payment Systems Regulator.
17. The Fintech Times.
18. UK payment firms push back on APP fraud refund plan (finextra.com).
19. Digital fraud attack rate in Singapore higher than APAC average: Cybercrime report - CNA (channelnewsasia.com).
20. Singapore Takes Aim At APP Fraud (vixio.com).
21. TODAYOnline.
22. FICO.
23. LexisNexis.
24. Payment Systems Regulator.
25. Payment Systems Regulator.
26. UK Finance, Annual Fraud Report 2023 (The "almost £100 million" figure is calculated from U.K. Finance data for 2022 in which £485.2 million was lost to APP fraud. Based on TSB's percent increase in detection and scam payments prevented, £97 million would be saved across the banking sector based on latest UKF data).

To learn more **contact one of our Mastercard Real-Time Payments experts** → **Visit our website** →

©2025 Mastercard | All Rights reserved
Mastercard is a registered trademark, and the circles design is a trademark, of Mastercard International Incorporated.