International Practices in Mitigating Faster Payments Fraud

Fasterpaymentscouncil.org

December 2024

Table of Contents

I. Introduction

Faster Payments play a crucial role in international commerce by facilitating transactions between individuals, entities, and financial institutions (FIs). However, the increasing volume and complexity of transactions also present challenges in fraud prevention. This report will explore anti-fraud controls for faster payments, including mitigation strategies and examples of measures implemented by various countries to prevent fraud.

In the first quarter of 2024, the U.S. Faster Payments Council (FPC) Fraud Work Group published "Faster Payment Fraud Trends and Mitigation Opportunities"[1]. This publication provided updates on the evolving U.S. landscape and identified opportunities to improve fraud mitigation, including gaps in mitigating faster payments fraud. This report aims to explore international lessons learned that may be applied to the U.S. market.

The FPC Fraud Work Group completed research on fraud risk controls across different faster payment networks and identified six common fraud risk strategies being used internationally. The work group analyzed these risk controls in different markets and report on leading practices to fight faster payments fraud.

To combat fraud in payments, financial institutions, networks, regulatory bodies, and other stakeholders can implement various mitigation strategies. These strategies can be broadly categorized as:

Category	Definition
Enhanced Authentication	Multi-factor authentication and/or biometric verification, which strengthens account security and prevents unauthorized access.
Transaction Monitoring	Advanced analytics and machine learning algorithms to detect suspicious patterns and anomalies in transactions in real-time and retrospectively.
Confirmation of Payee (CoP)	Service to verify the identity of customers and conduct thorough due diligence to mitigate scams and errors. Note, CoP can occur upfront when an alias is created or when an account holder adds a new payee, or each time a transaction is initiated. CoP systems for every transaction are typically expensive and serve to reduce "fat finger" errors vs. preventing authorized payments scams. Despite CoP controls being in place, fraudsters use social engineering techniques to bypass CoP checks by manipulating and deceiving victims into sending funds to accounts they control. For example, in 2020 when CoP was rolled out in the UK, reported cases of authorized payments scams rose 22%.[2]

Pre-Transaction Collaboration and Information Sharing	Intelligence sharing among stakeholder institutions.
Post-Transaction Collaboration and Information Sharing	Continued integration and cooperation between parties after the payment completion including working together quickly on fraud claims and reporting validated fraud to enforcement authorities.
Enhanced Consumer Protection	Advanced measures and practices such as liability shift to safeguard reasonably vigilant customers from fraudulent activities.

Implementing a comprehensive approach that combines these strategies is essential for effectively mitigating payments fraud. The following section describes the capabilities that select countries use and the learnings the United States could draw from those experiences.

A note on fraud and scams:

Fraud generally involves deliberate deception for financial gain, often targeting institutions and individuals through unauthorized transactions by account takeovers, identity theft, or card counterfeiting. Scams generally involve deceptive schemes designed to mislead individuals into providing personal information and authorizing financial transactions. Many countries have laws and regulations to combat both fraud and scams and approaches can vary significantly based on legal frameworks, regulatory practices, consumer protections or levels of technological advancement.

II. Singapore

Singapore's FAST®[4] is a real-time payment system that allows customers of participating banks to transfer funds. PayNow®, a complementary overlay service, is built on the FAST system. Singapore's fraud prevention framework focuses on pre- and post-transaction collaboration and information sharing, consumer notification and education, and transaction monitoring. It aims to protect consumers from unauthorized transactions but does not address scams.

A. Shared Responsibility Framework

Singapore's proposed "Shared Responsibility Framework"[5] (SRF), published October 2023 by the Monetary Authority of Singapore (MAS)[6] and Infocomm Media Development Authority (IMDA)[1], sets out a framework for sharing responsibility for losses from scams among FIs, telecommunication operators (Telcos), and consumers. Specifically, it addresses unauthorized transactions resulting from phishing scams, in which consumers are tricked into providing credentials on a fraudulent digital platform. If FIs or Telcos fail to meet specified anti-scam duties, they are expected to compensate the victims.

Liability is determined via a "waterfall approach," with FIs primarily responsible, followed by Telcos, and finally, consumers if both institutions have fulfilled their duties. The claim process includes investigation, outcome, and appeals process for consumers. Financial institutions have various responsibilities, including:

- Providing prompt real-time alerts to consumers based on monitoring of suspicious activities such as unusual transactions.
- Implementing filters to block/flag SMS messages that are likely scam attempts such as phishing attempts.
- Establishing cooling-off periods for new security tokens for high-risk transactions.
- Sending immediate transaction alerts for all outgoing transactions.
- Utilizing advanced fraud detection systems to quickly identify unauthorized transactions.
- Maintaining verified and secure communication channels.

Telcos also have various responsibilities, including implementing robust anti-scam filters to screen out phishing links sent via SMS, blocking SMS messages from unknown or unverified sources, partnering with FIs to share pertinent information such as trends and conducting consumer education campaigns.

It is important to note that this framework excludes authorized payment scams, such as romance scams or malware scams, which are acknowledged to require a different approach. Consumers are advised to file a claim with the Financial Industry Disputes Resolution Centre Ltd.[7] This independent institution resolves consumer financial disputes through mediation, a more cost-effective alternative to going to court.

B. Anti-Scam Centre Robotic Process Automation

The Singapore Police's Anti-Scam Centre[8] (ASC) collaborated with four banks to leverage Robotic Process Automation to detect job, investment, and other scams. The ASC promptly alerts potential victims through SMS notifications. A pilot conducted in 4Q 2023 disrupted over 5,300 scams and prevented more than $69 million in losses.[9]

C. Singapore Police Force Weekly Scam Bulletin

The police release a weekly scam bulletin[10] that highlights various trends, such as social media scams. These scams include misleading advertisements for discounted items that lead to phishing sites, fake fees for phony prizes, investment scams offering non-existent opportunities, and fraudulent bank promotions promising high-interest deposits.

A. NIBSS

The Nigeria Inter-Bank Settlement System[11] (NIBSS) is an ACH operator that provides the infrastructure for automated processing, settlement of payments, and fund transfer instructions between banks and other FIs in the country. NIBSS plays a crucial role in facilitating electronic payments, such as interbank transfers and direct debits. It also oversees various payment systems and implements initiatives to enhance the efficiency and security of financial transactions in Nigeria. It was incorporated in 1993 and is owned by all licensed banks, including the Central Bank of Nigeria (CBN).

In 2015, the Central Bank of Nigeria issued a circular mandating that NIBSS offer behavior, pattern monitoring solutions, and implement hold/block controls on transactions suspected to be fraudulent.[12] Banks can build this solution themselves or outsource this function. NIBSS offers an enterprise anti-fraud solution for this purpose, in addition to the central monitoring service.

As a pivotal player in the financial ecosystem, NIBSS recognizes the imperative of safeguarding transactions and ensuring the integrity of the payments landscape. Key elements of NIBSS's fraud mitigation strategy include:

1. **Multi-layered Authentication and Verification**: NIBSS employs a robust multi-layered approach to verify the identity of users and mitigate the risk of unauthorized access or transactions. To address the need for speed and transparency in platform integration and certification, NIBSS created an Industry Sandbox in 2020. In 2021, to improve industry efficiency for KYC (Know Your Customer), NIBS launched a centralized Address Verification service. This service provides access to all NIBSS services in a single suite and allows FIs to proactively carry out KYC to verify their customers respectively.

2. **Transaction Monitoring**: Real-time transaction monitoring systems are leveraged to detect suspicious activities promptly. Through advanced analytics and machine learning algorithms, NIBSS can identify anomalous patterns indicative of fraudulent behavior.

3. **Collaborative Partnerships**: NIBSS collaborates closely with FIs, regulatory bodies, and law enforcement agencies to exchange intelligence, share best practices, and coordinate responses to emerging threats. For example, The Bank Verification Number (BVNs) Watch-list[13] is a database of bank customers identified by their BVN who have been involved in confirmed fraudulent activities. The database is hosted by NIBSS, which is responsible for updating the database using watch-list reports submitted by banks.

   NIBSS is also accountable for providing banks with a portal for the verification of watch-list individuals and an API for banks to integrate their systems with the watch-list database for online verification of watch-list individuals at the time of transaction.

3. **Education and Awareness**: Recognizing the critical role of education in combating fraud, NIBSS invests in initiatives to raise awareness among stakeholders, including consumers, merchants, and FIs. By promoting a culture of vigilance and providing guidance on security best practices, NIBSS empowers individuals to safeguard their transactions effectively.

Through these concerted efforts, NIBSS endeavors to foster trust, reliability, and security in the payments landscape, ultimately facilitating seamless and secure transactions for all stakeholders.

IV. UK

Given that the UK faster payments systems have been live for over 15 years, fraud and scam typologies have evolved over that time, and so have the countermeasures implemented to mitigate these risks. Some industry-level mitigation strategies and corresponding capabilities, like 3DS authentication and confirmation of payee, are regulatory-driven changes. These protections have helped put the UK in a leading position regarding industry-level fraud and scam mitigation strategies.

A. Enhanced Authentication

By January 2018, with the introduction of the PSD2 regulation[14], all FIs in the UK and EU member states were required to implement multifactor authentication, such as biometric verification,. One of the main objectives of this PSD2 requirement was to enhance account security and prevent unauthorized access to combat a rise in account takeover across Europe. Since 2018, UK banks have successfully integrated various capabilities into their defenses to introduce additional authentication methods. In all digital journeys, multifactor authentication is used, whether through biometrics, passwords, device authentication, or other ID verification. One-time passcodes are gradually being phased out due to the risk of individuals inadvertently providing them to fraudsters, particularly in Authorized Push Payments (APP). Many institutions use identity verification technology vendors, which have been quite effective in helping FIs protect against unauthorized fraud. While consortium data is being used in this area, one significant gap is using Telco data in decision-making, which could enhance defenses. There are aspirations in the UK to improve data sharing, which presents the potential for this.

B. Centralized Transaction Monitoring and Collaboration and Information Sharing

As a result of implementing stronger customer authentication capabilities required under PSD2, fraudsters have shifted focus to target consumers utilizing social engineering scams to manipulate or deceive the payer into making an authorized payment to the fraudster. The increase in these authorized payment scams in the UK, known as APP, has led to changes in reimbursement rules introduced by the Payments Services Regulator, which came into effect in October 2024. These rules ensure that victims will be fully reimbursed in most cases, except in instances of negligence.

As a result, financial institutions are increasingly focused on preventing these scams. However, since the defensive measures put in place for unauthorized payment fraud[15] can be bypassed by the account holder (considering it is their account, biometrics, and passwords), many layers of defense are breached. Banks must explore more innovative approaches. Banks and the government have determined that "enhanced data sharing" is the best path to success. The government is encouraging the technology sector and telecommunication companies to take shared responsibility in addressing the issue, but it has not yet legislated these industries. This means that banks are exploring industry-wide solutions, looking beyond their own operations.

One successful example where the industry has demonstrated collaboration and information sharing is utilizing network level transaction data from faster payments to develop a centralized transaction monitoring capability developed by Mastercard®, called Consumer Fraud Risk.[16] The solution leverages network-based data analytics such as machine learning applied to faster payments transaction data to identify suspicious transactions prior to the funds leaving the account. Combining a network view and understanding payments and account behavior with the bank's deeper understanding of the customer accounts, the participating banks have been able to significantly increase detection rates while reducing false positives.

C. Confirmation of Payee

Confirmation of Payee (CoP) entails verifying the receivers and conducting thorough due diligence to mitigate the risk of identity theft and account takeover. In the UK, CoP validates that the name on the beneficiary account matches the one the sender provides for the beneficiary. The service provides a layer of comfort to the sender that the money is going to their intended payee. This is why the service is being rolled out beyond the initially mandated nine large banks (often called CMA9) by the Competition and Markets Authority[17] in the UK. Confirmation of Payee has reduced misdirected payments; however, the impact on fraud and scams has been limited. Scammers have worked out ways to manipulate or create accounts to fit and still coerce victims into sending money willingly.

V. Australia

The Reserve Bank of Australia[18] and its Payments System Board[19] (PSB) launched the New Payments Platform®[1] (NPP) in 2018. As of Q3 2023, 110 banks, credit unions, building societies, and fintech companies participate in the NPP.

With a high concentration in the market's banking sector, proven anti-fraud strategies and technologies have been implemented with high efficiency relative to more fragmented markets like the United States. Moreover, Australian banks have demonstrated the ability to take an industry-led approach to collaborating in the fight against financial crime which the United States would do well to emulate.

A. Confirmation of Payee

1. The banking industry has taken the initiative to develop and implement a new $100 million CoP system, which will incorporate name-checking technology to verify payee details and prevent customers from falling victim to scams. This system will alert customers if they are about to pay unintended recipients and will provide increased warnings about potential risks. The system is in development and expected to roll-out in 2025.

2. The Commonwealth Bank has introduced NameCheck®[21,22], a security tool designed to verify the accuracy of account details entered by CBA customers when making their first payment through NetBank, the CommBank app, or CommBiz. Based on the bank's payment data, NameCheck will confirm whether the account details are correct.

B. Collaboration and Information Sharing

1. **Inter-bank collaboration**: Australian banks have joined forces to launch a new Scam-Safe Accord[23] to deliver a higher standard of protection for customers and put scammers out of business in Australia. This Accord, between Australia's community-owned banks, building societies, credit unions and commercial banks is a comprehensive set of anti-scam measures across the entire industry.

2. **Post-transaction intelligence sharing**: The Scam-Safe Accord includes a major expansion of intelligence sharing across the sector. By mid-2024, banks will have acted on scam intelligence from the Australian Financial Crimes Exchange[24] (AFCX) and join the Fraud Reporting Exchange. The AFCX is the primary channel through which the public and private sector will coordinate their intelligence and data-sharing activities for the investigation and prevention of financial and cybercrime. By sharing information such as suspicious accounts and transactions, analyses of those activities, and evidence-based insights, AFCX members create a powerhouse of financial and cybercrime intelligence that takes the fight beyond simply policing transactions and investigating irregularities. Several of the country's leading banks have been actively sharing suspicious accounts and transactions with AFCX for years and are working to expand their membership and include scams in the exchange. AFCX is an independent, not-for-profit organization that was formed by the four major Banks to assist businesses combat financial-related crimes. It operates independently of government, law enforcement and its members, although it is funded by its members.

National Anti-Scam Centre[25] (Scamwatch): The National Anti-Scam Centre, run by the Australian Competition and Consumer Commission[26] (ACCC), brings together experts from government, law enforcement and the private sector to disrupt scams before they reach consumers.

VI. India

Real-time payments accounted for 266.2 billion transactions globally in 2023, a year-over-year growth of 42.2%. Additionally, India is by far the largest real-time payment network in the world. With 129.3 billion real-time payments in 2023, India accounts for a staggering 44.6% of all real-time payments. Consequently, India also faces significant fraud challenges, which it aims to address with current and future risk controls.[27]

A. Enhanced Authentication

India's Unified Payments Interface® (UPI) instant payments system currently uses enhanced authentication for all its real-time payments with One-Time Passwords ("OTPs") using a simple SMS or "Additional Factor Authentication" ("AFA"). However, the UPI network is exploring the expansion of authentication methods to include behavioral biometrics, location and historical information, digital tokens, and in-app notifications, all aimed at improving security.

B. Transaction Monitoring

Financial institutions currently use advanced fraud monitoring and detection capabilities, but there is still much work to be done to reduce fraud and be more proactive. The number of fraud cases in Indian banks surged in FY24 to 36,075 from 9,046 in FY22, a nearly 300% increase, while the value involved dropped by 46.7%. Most fraud occurred in digital payments, but the highest value fraud were in loan portfolios, with public banks contributing the most by value.[28] It is important to note that the number of cases is currently estimated to be under-reported. Therefore, improving collaboration and information sharing will enhance reporting, visibility across UPI, and transaction monitoring at payment providers.

C. Confirmation of Payee

UPI is set to introduce new measures in the coming year to have CoP within their network. The initiative will comply with the new regulatory requirements set out in Digital Personal Data Protection Act[29] in 2023 to ensure privacy is kept top-of-mind for organizations.

D. Collaboration and Information Sharing

The Reserve Bank of India currently requires commercial banks and non-bank Prepaid Payment Instrument (PPI) issuers to report fraud into the Central Payments Fraud Information Registry. Under the Reserve Bank of India's (RBI)'s Utkarsh 2.0[30] initiative, the Central Payments Fraud Information Registry will be expanded to require post transaction fraud reporting from other payment providers like local banks, cooperatives, regional rural banks, and non-scheduled urban cooperative banks. This effort aims to create a more comprehensive and robust fraud reporting system across various FIs.

VII. South Africa

BankservAfrica®[31] (BSA), South Africa's ACH operator, has a Fraud Intelligence[32] service, which provides banks pre-transaction descriptive statistics on all interbank payments (inbound and outbound) touching their FI. The Fraud Intelligence service reports information from all payment systems operated by BSA, including the batch system (EFT), PayShap®[33] (the instant payment system that went live in March 2023), and TCIB®[34], a cross-border instant payment systems serving the Southern Africa Development Community[35] (SADC) for South African Rand-denominated remittances.[36]

A. Collaboration and Information Sharing

Fraud Intelligence scans all payment transactions, assigns a risk score based on defined rules, and alerts the FIs that subscribe to the value-added service. BSA has now allowed beneficiary FIs to access the tool's information. Sending FIs may use this information to alert the sending customers of the potential for fraud but are not obligated to do so.[37] The Fraud Intelligence service does not stop or prevent a given transaction from being made, regardless of its scoring.

The Southern African Fraud Prevention Service is a database of known fraudsters operating within the SADC region.

B. Confirmation of Payee

BSA also has a CoP-like service called the Account Verification Service. It allows sending customers to verify the details of the beneficiary prior to sending a payment.[38]

VIII. Brazil

In just three short years, Brazil's PIX® has become the world's second largest real-time payments market. In 2023, PIX processed just over 37 billion real-time payments; that is over 75% of all Latin America's real-time payments. But with this rapid growth, PIX has also seen its fair share of unique fraud risks. Street robberies and late-night kidnappings increased dramatically, forcing PIX to tighten overnight limits and launch solutions such as PIX Precautionary Block, which allows suspending the PIX transactions for 72 hours to allow time for investigations to occur and assess risk.

A. Enhanced Authentication

PIX itself do not cover authentication/ID&V. The user is already logged into the Bank or Payment Institution application, so the ID&V part is fully based on the requirements to be a financial player in Brazil. Thus, each member's multi-factor authentication and/or ID&V are based on their own risk appetite. There are currently no plans for the regulator to intervene in this space.

B. Transaction Monitoring

Transactional Fraud prevention for PIX is also the responsibility of the institutions. Financial institutions have an obligation to monitor, but it is not specific to the PIX channel itself.

C. Confirmation of Payee

PIX has had CoP from day one. The central infrastructure has this information, and it allows the sender to see the actual name of the payee. An update to the system now allows for PIX transactions that are from within the same institution to bypass this requirement and the verification can be done faster and from within the institution.

D. Collaboration and Information Sharing

The Central Bank of Brazil has created a shared adverse database for accounts linked to fraud and money mules. This information will potentially allow for the tracing of funds across multiple layers to attempt to trace and recover funds.[39]

IX. Eurozone

There are also newer mitigation efforts, such as EBA Clearing. EBA Clearing is the private sector pan-European ACH that covers the Eurozone market and operates several payment systems, including Euro1 (high-value, comparable to CHIPS in the US), STEP2 (batch ACH), and RT1 (instant payments).

A. Collaboration and Information Sharing

In March 2024, the FPAD (Fraud Pattern and Anomaly Detection) value-added service was launched. FPAD uses data from STEP2 and RT1 to detect and prevent fraud as well as provide fraud intelligence to payment service providers (PSPs). FPAD has three functionalities: an IBAN name check, a prevent module, and a detection module.

B. Confirmation of Payee

FPAD's CoP service allows sending PSPs to check the name associated with the recipient's IBAN prior to payment initiation.

C. Transaction Monitoring

FPAD's prevention modules assess the risk associated with recipient accounts and transactions prior to payment message submission whereas the detection modules perform post-transaction investigation. FPAD's modules are meant to supplement PSP efforts and to integrate seamlessly with PSP data processing.[40]

The Euro Banking Association (a separate legal entity from EBA Clearing) recently released its fraud and scam taxonomy to help with data issues related to reporting fraud in the wider Eurozone.[41] FPAD does not stop payments from being made.

X. Conclusion

The following table illustrates the spectrum of implementation for each strategy ranging from advanced ● to no or little implementation ○.

Strategy	Singapore	Nigeria	UK	Australia	India	South Africa	Brazil
Required Enhanced Authentication: MFA, including biometrics	○	●	●	●	●	○	◔
Transaction Monitoring: advanced analytics and ML to detect anomalies	◔	●	●	◔	◔	●	◔
Confirmation of Payee: verify confirmation of recipient along with due diligence to prevent scams and errors	○	○	●	◕	◕	●	●
Pre-Transaction Collaboration and Information Sharing: intelligence sharing among stakeholder institutions	◔	●	●	◐	○	●	◔
Post-Transaction Collaboration and Information Sharing: intelligence sharing among stakeholder institutions	◕	●	●	●	◕	●	◐
Enhanced Consumer Protection: protect customers from fraud	◕	○	●	○	○	○	○

XI. Comparison to the United States

The United States has multiple faster payment options, and so a comparison of overseas faster payment systems to the United States requires looking at each of the U.S. systems. In this report, four are considered:

- **Zelle®**, a person-to-person system operated by Early Warning Services, provides immediate messaging, and funds availability but delayed settlement.

- **Debit Push**, offered by Visa and Mastercard on their debit card rails primarily to large volume business originators, provides immediate funds availability but delayed settlement.

- **RTP®**, offered by The Clearing House (TCH), uses ISO20022 messaging to provide both immediate funds availability and settlement.

- **FedNow® Service**, an instant payments infrastructure which uses ISO20022 messaging standards, provides immediate funds availability and settlement.

Note that **Same Day ACH**, also offered by both TCH and the Fed, provides same-day funds availability and settlement, but it is not considered here.

Referring to the chart below, the U.S. faster payment systems implement varying degrees of the fraud mitigation strategies employed by overseas payment systems.

- **Enhanced Authentication:** Federal Financial Institutions Examination Council (FFEIC) guidelines point out the need for banks to have enhanced authentication methods such as multi-factor authentication (MFA) for higher risk situations, and U.S. instant payment network rules require the use of MFA or equivalent controls.

- **Transaction Monitoring:** The card networks, Zelle, RTP, and FedNow Service all require FIs to monitor transactions, and to report fraud-related payments and collaborate in resolving them. Zelle and the card networks also directly monitor transactions. The FedNow Service offers each Participant the option to establish their own negative list for the network to reject transactions either coming from or to specific accounts based on the Participant's negative list.

- **Confirmation of Payee:** Zelle provides a name match, but not necessarily an account verification, each time a consumer adds a payee to their Zelle directory. RTP rules require that sending FIs provide consumer senders with the name of the receiver, or reasonable assurance that the receiver is the sender's intended recipient of funds. Business originators using Debit Push on card rails can confirm certain accounts at the time of receiver enrollment.

- **Pre-Transaction Information Sharing:** Zelle provides sending FIs with real-time statistics on proposed receiver accounts, including any fraud reports, which have been demonstrated to help identify riskier receivers. Sending FIs can incorporate this data in fraud decisioning before initiating an instant payment Debit Push leverages existing pre-transaction reporting (e.g., compromised card) to enable sending institutions to evaluate risks associated with beneficiary cards prior to sending funds.

- **Post-Transaction Collaboration:** All faster networks reviewed here mandate fraud reporting and collaboration among participating FIs to resolve cases. Comparing the U.S. requirements for fraud reporting to enforcement authorities is complex and beyond scope of this report.

- **Enhanced Consumer Protection:** The United States operates under the EFTA/Reg E regulatory frameworks, which require sending FIs to reimburse consumer account holders for unauthorized payments. However, in cases where the sender authorizes a payment, but later claims they were duped by the receiver, the fraud loss typically remains with the sender. Zelle has started to require receiving FIs reimburse senders for certain qualifying imposter scams, even when the sender authorized the payment.

Strategy	Debit Push	FedNow Service	RTP	Zelle
Enhanced Authentication: MFA, including biometrics	●	●	●	●
Transaction Monitoring: advanced analytics & ML to detect anomalies	●	○	○	◕
Confirmation of Payee: verify confirmation of recipient along with due diligence to prevent scams and errors	◐	◐ (no name)	◐	◕
Pre-Transaction Collaboration and Information Sharing: intelligence sharing among stakeholder institutions	◐	○	○	◕
Post-Transaction Collaboration and Information Sharing: intelligence sharing among stakeholder institutions	◕	◔	◔	◕
Enhanced Consumer Protection: protect customers from fraud	◐	◐	◐	◐

The Federal Reserve's *Scams Information Sharing Industry Work Group Recommendations*[42] and the *ScamClassifier*[43] model, published in the Summer of 2024, offer significant improvements for combating scams in U.S. payments. The scams information sharing industry work group advocates for an industry-wide information exchange to facilitate real-time scam intelligence sharing. This would allow institutions to better detect and prevent scams across payment types. The *ScamClassifier* model complements this by providing a standardized approach to classify scams based on deception methods, independent of the payment type or channel. It helps organizations improve scam detection, reporting, and mitigation, ensuring consistent application across the industry. Together, these initiatives are expected to enhance collaboration and strengthen the U.S. payments system's ability to address evolving scam tactics and strategies.

One example of a proposed real-time industry-wide information sharing capability is being developed by the American Bankers Association called the Fraud Indicator Exchange (FIX). The goal of the FIX is to create a capability that allows a consortium/association of banks to share in near real-time, away or "off-us" accounts that have been reported and identified as engaging in potentially fraudulent activity. Program participants can add these accounts to internal "friction lists" that allow them to check if any outgoing transactions are going to an identified account. If there is a match, an institution can perform additional due diligence to see if the transaction should be completed with the overall goal of stopping the flow of funds to accounts that are actively being used by criminals in their scams. This program leverages the information sharing mechanisms provided under the Patriot Act's Section 314b and plans to have an operational pilot in place in early 2025.[44]

XII. Conclusion

The examination of international fraud prevention strategies in faster payments reveals several leading practices. Countries like the UK, Singapore, and Australia demonstrate the effectiveness in mitigating fraud with multi-factor authentication, real-time transaction monitoring, and to a lesser degree confirmation of payee systems. Collaborative efforts to share fraud-related data are bearing fruit in some overseas jurisdictions, and two jurisdictions (UK, Singapore) are working with new shared liability frameworks.

The U.S. payments ecosystem may collectively wish to consider emulating some of these overseas practices, e.g., developing comprehensive strategies, continually enhancing authentication protocols, and fostering greater collaboration among financial institutions such as public private partnerships for intelligence sharing. Implementing these strategies could help further mitigate and address fraud risks in the evolving landscape of faster payments.

Acknowledgements

Fraud Work Group

Thank you to the members of the FPC Fraud Work Group (FWG), sponsored by Nasdaq Verafin, who contributed to this report.

FWG Leadership

Lee Kyriacou (Chair), (formerly with) The Clearing House Payments Company, LLC
Erik Provitt (FPC WG Facilitator), Guidehouse

FWG Contributors

Marc Trepanier, ACI Worldwide
Neil Kumar, Alloya Corporate FCU
Paul Benda, American Bankers Association
Andrew Gomez, Andrew Gomez Payments Consulting
Jens Seidl, Currency Research USA Corp
Alex Niu, DataVisor
Sandra Desautels, Guidehouse
Charlie Trainor, Interac Corp.
Rene Perez, Jack Henry & Associates
Satya Vandrangi, JP Morgan Chase
Liam Cooney, Mastercard International
Todd Porter, MITRE
Kathleen Shea, NEACH (The New England ACH Association)
Deborah Baxley, PayGility Advisors LLC
Anthony Serio (Editor), Sphere Laboratories, Inc.
Nicole Sedita, Zumigo Inc

About the U.S. Faster Payments Council and the Fraud Work Group

The U.S. Faster Payments Council (FPC) is an industry-led membership organization whose vision is a world-class payment system where Americans can safely and securely pay anyone, anywhere, at any time and with near-immediate funds availability. To further this vision, the FPC established the Fraud Work Group to collaborate with payments stakeholders to identify, prevent, and mitigate faster payments fraud.

References

[1] Faster Payments Council. (2024, January). *Bulletin.01: Faster Payments Fraud Trends and Mitigation Opportunities.* https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

[2] UK Finance. (2021*). Fraud – the Facts 2021.* https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf.

[3] The Association of Banks in Singapore. (n.d.). *Consumer Banking – Faster and Secure Transfers.* Retrieved December 16, 2024 from https://www.abs.org.sg/consumer-banking/fast.

[4] Monetary Authority of Singapore. (2023, October). *Consultation Paper on Proposed Shared Responsibility Framework.* https://www.mas.gov.sg/-/media/mas-media-library/publications/consultations/pd/2023/srf/consultation-paper-on-proposed-shared-responsibility-framework.pdf.

[5] Monetary Authority of Singapore. (n.d.). Retrieved December 16, 2024 from https://www.mas.gov.sg/.

[6] Infocomm Media Development Authority. (n.d.). Retrieved December 16, 2024 from https://www.imda.gov.sg/.

[7] FIDRec. (n.d.). Retrieved December 16, 2024 from https://www.fidrec.com.sg/.

[8] Singapore Police Force. (2024, January 9). *Anti-Scam Centre and Four Partnering Banks Utilize Technology in Three-And-A-Half-Long Joint Operation, Successfully Preventing Scam Losses of Over $69.43 Million for More Than 15,000 Victims.* https://www.police.gov.sg/Media-Room/News/20240109_anti_scam_centre_and_four_partnering_banks_utilize_technology.

[9] Singapore Police Force. (2024, July 5). *More Than 9,800 Potential Scam Victims Alerted in Joint Operation Between Anti-Scam Centre and Six Partnering Banks.* https://www.police.gov.sg/media-room/news/20240705_more_than_9800_potential_scam_victims_alerted_in_joint_operation_between_anti_scam_centre.

[10] Singapore Police Force. (n.d.). *Scams.* Retrieved December 16, 2024 from https://www.police.gov.sg/Media-Room/Scams-Bulletin.

[11] NIBSS. (n.d.). Retrieved December 16, 2024 from https://nibss-plc.com.ng/.

[12] NIBSS. (n.d.). *Media Updates.* Retrieved December 16, 2024 from https://nibss-plc.com.ng/how-cbn-revolutionized-payment-systems-in-nigeria/.

[13] Central Bank of Nigeria. (2017, October 18). *Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry.* https://finclusion.org/Out/2017/BPSD/Circular%20on%20the%20Regulatory%20Framework%20for%20BVN%20%20Watchlist%20for%20Nigerian%20Financial%20System.pdf.

[14] European Central Bank. (201, March). *The revised Payment Services Directive (PSD2) and the transition to stronger payments security.* https://www.ecb.europa.eu/press/intro/mip-online/2018/html/1803_revisedpsd.en.html.

[15] Faster Payments Council. (2024, January). *Bulletin.01: Faster Payments Fraud Trends and Mitigation Opportunities.* https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

[16] Mastercard. (n.d.). *Consumer Fraud Risk.* Retrieved December 16, 2024 from https://developer.mastercard.com/product/consumer-fraud-risk/.

[17] GOV.UK. (n.d.). *CMA: Competition and Markets Authority.* Retrieved December 16, 2024 from https://www.gov.uk/government/organisations/competition-and-markets-authority.

[18] Reserve Bank of Australia. (n.d.). *News and Announcements.* Retrieved December 16, 2024 from https://www.rba.gov.au/.

[19] Reserve Bank of Australia. (n.d.). *Payments Systems Board.* Retrieved December 16, 2024 from https://www.rba.gov.au/about-rba/boards/psb-board.html.

[20]] Reserve Bank of Australia. (n.d.). *The New Payments Platform.* Retrieved December 16, 2024 from https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/.

[21] Commonwealth Bank. (2023, November 27). *CBA Rolls Out NameCheck availability to leading industry names.* https://www.commbank.com.au/articles/newsroom/2023/11/cba-namecheck-availability-bendigo-satori.html.

[22] Emanuel-Burns, Cameron. (2024, May 30). Commonwealth Bank of Australia to pilot NameCheck solution on JP Morgan's Liik network. *Fintech Futures.* https://www.fintechfutures.com/2024/05/commonwealth-bank-of-australia-to-pilot-namecheck-solution-on-jp-morgans-liink-network/.

[23] Australian Banking Association. (n.d.). *Keeping Australia Scam Safe.* Retrieved December 16, 2024 from https://www.ausbanking.org.au/scam-safe-accord/.

[24] Financial Crimes Exchange. (n.d.). *Joining Forces to Fight Financial and Cyber Crime.* Retrieved December 16, 2024 from https://www.afcx.com.au/.

[25] Australian Government ScamWatch. (n.d.). *Know when to stop and check – stay safe from scams.* Retrieved December 16, 2024 from https://www.scamwatch.gov.au/.

[26] ACCC. (n.d.). Retrieved December 16, 2024 from https://www.accc.gov.au/.

[27] The Economic Times. (2024, June 1). *How RBI is looking to curb payment frauds in FY25.* https://bfsi.economictimes.indiatimes.com/news/policy/how-rbi-is-looking-to-curb-payment-frauds-in-fy25/110608802.

[28] The Economic Times. (2024, May 311). *Bank frauds up nearly 300% in last two years, digital frauds up 708%: RBI.* https://economictimes.indiatimes.com/industry/banking/finance/banking/bank-frauds-up-nearly-300-in-last-two-years-digital-frauds-up-708-rbi/articleshow/110555108.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[29] Meity.gov. (2023, August 11). *The Digital Personal Data Protection Act, 2023.* https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

[30] The Economic Times. (2023, May 8). *Utkarsh 2.0 RBI's strategy framework – key points to know.* https://economictimes.indiatimes.com/markets/stocks/news/utkarsh-2-0-rbis-strategy-framework-key-points-to-know/articleshow/100067996.cms?from=mdr.

[31] BankservAfrica. (n.d.). Retrieved December 16, 2024 from https://www.bankservafrica.com/website/.

[32] SAFP. (n.d.). Retrieved December 16, 2024 from https://www.safps.org.za/.

[33] PayShap. (n.d.). Retrieved December 16, 2024 from https://www.payshap.co.za/#/home.

[34] BankservAfrica. (n.d.). *Transactions Cleared On An Immediate Basis (TCIB).* Retrieved December 16, 2024 from https://www.bankservafrica.com/website/services/transactions-cleared-on-an-immediate-basis.

[35] SADC. (n.d.). Retrieved December 16, 2024 from https://www.sadc.int/.

[36] BankservAfrica. (n.d.). *Fraud Intelligence.* Retrieved December 16, 2024 from https://www.bankservafrica.com/website/.

[37][38] SAFPS. (n.d.). Retrieved December 16, 2024 from https://www.safps.org.za/.

[39] FFIS. (2024, January). *The case for the G20 cross-border payments reform 'Roadmap' to embed economic crime security by design.* https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_-_payments_policy_discussion_paper_2_-_g20_payments_roadmap_and_economic_crime_security__.pdf.

[40] EBA Clearing. (2023, September 14). *EBA Clearing issues specifications and runs analytical pilot for pan-European fraud pattern and anomaly detection.* https://www.ebaclearing.eu/news-and-events/media/press-releases/14-september-2023-eba-clearing-issues-specifications-and-runs-analytical-pilot-for-pan-european-fraud-pattern-and-anomaly-detection/.

[41] Euro Banking Association. (n.d.). *Expert Group on Payment Fraud-related Topics.* Retrieved December 16, 2024 from https://www.abe-eba.eu/market-practices-regulatory-guidance/expert-group-on-payment-fraud-related-topics/.

[42] The Federal Reserve. (n.d.). *Scams Information Sharing Industry Work Group Recommendations.* Retrieved December 16, 2024 from https://fedpaymentsimprovement.org/wp-content/uploads/scams-information-sharing-industry-work-group-recommendations.pdf.

[43] The Federal Reserve. (n.d.). *ScamClassifer^{SM} Model.* https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/.

[44] McCaffrey, Orla. (2023. November 28). ABA to launch information-sharing exchange to help banks fight fraud. *American Banker.* https://www.americanbanker.com/news/aba-to-launch-information-sharing-exchange-to-help-banks-fight-fraud.