Faster Payments Fraud Trends and Mitigation Opportunities

Bulletin.01

The Faster Payments Council (FPC) Fraud Work Group offers its first Bulletin[1] aimed at fostering safer user experiences and bolstering confidence and trust in faster payments.

Bulletin.01 discusses the previous Work Group's foundational work, updates on the evolving landscape, and identifies opportunities to improve fraud mitigation – including gaps in mitigating faster payments fraud.

In this edition:

Prior Work

From 2020 to 2022, the FPC's Fraud Information Sharing Work Group (FISWG) and Financial Inclusion Work Group (FIWG) conducted foundational work and published papers that focused on faster payments fraud:

- *Examining Faster Payments Fraud Prevention*[2]: In July 2020, the FISWG white paper outlined existing fraud schemes, including identity theft, account takeover, synthetic identity, and social engineering, as well as several other emerging fraud schemes. The FISWG analyzed industry data and real-life use cases to identify prevalent types of fraud and the associated attack vectors, examined challenges posed by the U.S. identity infrastructure, and considered emerging push payment scams. The report recommended implementing a range of technical and behavioral controls, including training, third-party vendor management, and regular testing and simulation exercises.

- *2021 Faster Payments Fraud Survey and Report*[3]: In August 2021, the FISWG conducted its inaugural faster payments fraud survey to gather quantitative and qualitative data from FPC members. Respondents identified account takeover, social engineering, and stolen credentials as the most common consumer fraud types. Invoice fraud, CEO impersonation fraud, and vendor/authority impersonation fraud were identified as the most common business fraud types. About half of respondents had implemented new technology controls and operational processes, stronger authentication, and/or AI based real-time decision making. The results of this survey, as well as a comparison between U.S. and global fraud trends, were published in March 2022.

- *Faster Payments and Financial Inclusion*[4]: In July 2022, the FIWG published a white paper that identified fraud as a barrier to full financial inclusion in faster payments. It concluded that the risk of losing scarce household funds to fraud posed a pain point and a barrier to faster payments usage, especially for the many U.S. households living paycheck to paycheck. The report recommended that entities in all parts of the payments ecosystem play a role in reducing fraud. The report noted that expanding financial inclusion would necessitate assistance and remedies for consumers who were tricked into sending money to a fraudster. Finally, the report cautioned that the use of biometric information for authentication and behavioral/pattern analysis may pose unique challenges for those persons who are underserved.

Current Trends and Mitigation Techniques

In recent years, the use of faster payment methods such as instant payment networks, same-day ACH, payment wallets, and push-to-card has significantly increased in the United States, including for person-to-person payments using services such as Zelle® and Venmo. As the volume of faster payments has grown, so has the associated fraud, which includes both authorized and unauthorized party payment fraud.

Authorized payment fraud. Authorized payment fraud occurs when an individual with the right to initiate a payment intentionally or unintentionally sends a fraudulent payment. There are different types of authorized payment fraud:

- Authorized push payment (APP) fraud, also known as authorized payment scams, where an authorized party is deceived or manipulated into sending a faster payment to a fraudster. This is the primary focus of this bulletin.

- Other types of authorized payment fraud include the following:
  - Where an authorized party intentionally attempts to defraud an organization.
  - Where an unauthorized party alters a previously authorized payment instruction.

APP fraud is increasing and is difficult for the payment industry to recognize since it is the actual bank account holder who is instructing the bank to send the payment. Common types of APP fraud impacting consumers include purchase scams, impostor scams, and investor scams. On the business side, examples include invoice scams and business email compromise.

The number of APP fraud cases involving consumers has grown significantly due to the increasing adoption of instant payment solutions and is expected to grow rapidly;[5] fraudsters are especially drawn to faster payments because, once they have induced the payer to send payment, they get quick and irrevocable access to funds.

To combat this problem, payment processors, banks, and other industry players are working to educate consumers about scams via multiple channels such as through targeted emails, advertising, pop-ups at the time of the transaction request, and social media posts.

In response to APP fraud targeting businesses, there has been an increased focus over the last several years on commercial customer education and awareness over the last several years. Enhanced Business workflow, quality assurance, and simulation testing have proved helpful; mitigation techniques such as multi-factor authentication have been implemented. As a result, compared to consumers, the incidence of APP fraud involving commercial customers[6] has received less media attention. However, the potential for obtaining large dollar payouts is greater with the commercial customer, making it attractive to fraudsters.

Mitigation techniques include using third-party data and public records to validate the consistency of personally identifiable information (PII) across different data sources. The use of alternate sources of public records such as property deed and tax records, voter registration, birth/death/marriage records, social security numbers, commercial licenses, and social media profiles have also helped to corroborate the authenticity of PII information. Technology solutions, such as machine learning tools and IP address tracking, help organizations analyze the validity of PII records and sources of transactions.

Unauthorized payment fraud. Unauthorized payment fraud, in which payments are initiated by parties that are not authorized to conduct them, is an ongoing risk. The most prevalent type of unauthorized payment fraud is account takeover (ATO), in which the fraudster gains unauthorized access to the account and the account holder's financial information.

Fraudsters have evolved their techniques by leveraging the latest technology to perpetrate increasingly sophisticated ATO attacks, including phishing, credential stuffing, fraudsters posing as bank staff, and SIM swapping, all at a much greater scale. The COVID-19 pandemic drove mass adoption of digital banking and e-commerce across all demographics, allowing fraudsters to access compromised credentials more easily from data breaches to attack large numbers of victims. Fraudsters launched large-scale ATO attacks utilizing bots and scripts to execute multiple attacks simultaneously.

To combat this issue, some large financial institutions and businesses have introduced education initiatives for both customers and employees, coupled with advanced fraud prevention strategies and tools that utilize machine learning and AI technology, including behavioral analytics and biometrics.

Let's Close the Gaps: Opportunities to Improve Fraud Mitigation

Despite the efforts made by faster payments stakeholders to mitigate fraud, gaps in fraud detection, prevention, and mitigation remain. These gaps present potential opportunities for further progress.

- Gap 1: Differing payment provider processes and technology. Narrowing differences in the implementation of faster payments processes and technology across the payment providers provides opportunities for more effectively identifying, preventing, and resolving fraudulent activities. Potential opportunities include:

    - Mitigation techniques and procedures. The mitigation techniques employed to identify and prevent unauthorized fraud in debit-pull payments differ from those effective in combating authorized fraud in credit-push scenarios. For example, the fraud focus for debit-pull card payments is on authenticating the card number, while in credit-push faster payments, the focus is on authenticating the account holder. Financial institutions transitioning to credit-push instant payments need to reposition their fraud mitigation approaches accordingly.

- **Standardized coding for fraud reporting.** The payments system could benefit from more standardized reason codes for reporting faster payment fraud scenarios and related disputes. Without a consistent and unified coding system, financial institutions face difficulties in promptly and accurately tracing the origins of fraudulent activities. For example, many cases of synthetic identify fraud are only attributed to credit losses. In addition to the difficulties in tracing fraud, the lack of standardized codes inhibits the development of training materials, targeted responses, and educational resources. Finally, absent a consistent coding system, disputes may be incorrectly routed or assigned to internal departments ill-equipped to manage them.

- **Identity verification/authentication.** Identity verification and authentication are critical components of real-time payments and fraud mitigation. While strong authentication controls and bank regulations are in place, there may be new fraud vectors to acquire user credentials or, once acquired, to execute account takeover payment fraud.

- **Confirmation of Payee (CoP) capability.** The U.S. market does not have a uniform capability for name checking and confirmation of payee. Pay UK and several UK financial institutions launched a name checking service for UK-based payments which provides customers (both personal and business) greater assurance that they are sending payments to the intended recipient, helping to avoid making accidental, misdirected payments to the wrong account holder, as well as providing some protection against fraud and scams. In the United States, several approaches are now in use:
    - Zelle provides the account holder name at the time a potential Zelle payer adds a new party to their Zelle payee directory.
    - An RTP® rule requires that a consumer sender be provided with the Receiver name (or reasonable assurance thereof) prior to sending an RTP Payment.
    - Third-party service providers offer step up verification services to bolster KYC and account opening processes, leveraging consortium data intelligence to help verify good users and bad actors before they can open an account.

- **Transaction monitoring.** There may be opportunities to shift more payment providers from continued reliance on manual transaction monitoring processes to more automated and real-time functionality. With increasing adoption of faster payments, on point solutions and manual transaction monitoring is unable to keep up with the fraudsters. Payment providers can consider leveraging automation for real-time, 24x7x365 activity monitoring and anomaly detection, including money movement and non-money movement activities. This includes improved pattern analysis and the inclusion of composite data from identity creation to transaction. Finally, behavioral analysis is another critical aspect that should become standard for transaction and activity monitoring.

- Gap 2: Limited information sharing. Improving information sharing across payments stakeholders also provides opportunities for more effectively identifying, preventing, and resolving fraudulent activities. There are known data sharing challenges, and ongoing industry efforts and advocacy to address each.

    - Fraud reporting. There are limited legal and regulatory requirements for fraud reporting, as well as differences between what is required of financial institutions versus non-bank payment providers. A lack of consistent and timely fraud reporting results in an incomplete picture of what is happening with fraud. Fraud reports identify bad accounts, and when combined with payment patterns of such accounts, help to build identifiers for future suspected bad accounts. Faster payment networks have taken some initial steps concerning fraud reporting within their networks. For example, Zelle requires unauthorized and scam (authorized) reporting, and both RTP and FedNow® have fraud reporting requirements as well. These network-driven efforts will assist in standardizing bank treatment of unauthorized consumer payments (for which there are legal requirements to address and if appropriate reimburse for consumer senders), as well as scams involving authorized payments or payments for commercial senders. However, there is more to be done.

    - Data definitions and standards. There is no required set of data definitions and standards for fraud reporting. Encouraging standardization could make data sharing easier, faster, and more effective. Some efforts are underway. The Federal Reserve's Fraud Definitions Work Group began tackling this issue several years ago, resulting in the Fed's Fraud Classifier℠[7] model of fraud categorization. Zelle, RTP and FedNow reporting use at a minimum the high-level classifications from the Fraud Classifier, if not the full granular classification details. A new Federal Reserve work group formed in 2023[8] is focused on developing an industry-recommended scams definition and detailing scam classifications. This is an area that needs further development.

    - Timely information sharing. Similarly, there is no uniform required timeframe for reporting fraud. Swiftly defining the nature of an attack and sharing this information across the market can strengthen collective defense against fraud, help resolve disputes, and better protect customers. There has been some activity to address this gap. For example, Zelle has added a requirement for quick reporting times, which faster payment networks seem likely to mirror. Yet there is more to be done.

    - Hesitancy to share. Banks, financial institutions, and payment providers typically have significant concerns about data sharing, including privacy concerns, anti-trust exposure, legal permission, liability,[9] reputational risks, and competitive considerations. To begin a dialogue in this area, the Federal Reserve has formed a work group on fraud information sharing, from which we can expect to see collaborative ways of reducing hesitancy to share while respecting appropriate limitations for sharing.

- **How to share.** There is a separate question on how relevant fraud data can be shared. Some work on this issue has begun. Zelle has started to offer Zelle Risk Insights, which provides real-time access to aggregated receiver statistics, to assist in fraud decisioning. Others are looking at ways to aggregate multiple sources of receiver information, including information directly from receiver financial institutions, without tripping legal or proprietary concerns of data providers. More solutions are needed.

- **Reporting to law enforcement.** Lastly, there are only limited legal or regulatory requirements to report fraud involving payments to law enforcement agencies. This does not impede the sharing of fraud-related information for decisioning purposes, but it may affect the ability to eliminate repeat offenders from synthetic identify and faster payment fraud. In other countries, it has been observed that law enforcement takes measures to entrap fraudsters.

Conclusion

Over the last several years, FPC work groups surveyed the payments fraud landscape and summarized mechanisms intended to prevent, detect, and mitigate faster payments fraud. Today, fraud requires constant vigilance as fraudsters become increasingly sophisticated.

While financial institutions and service providers have developed new methods to combat complex fraud schemes, stakeholders have two key opportunities to strengthen this collective effort:

1. Industry stakeholders can adopt common fraud-prevention related processes and technology. The range that exists today limits stakeholders' ability to adopt common industry best practices.

2. Industry stakeholders can improve information sharing practices. Nonexistent standards and norms prevent stakeholders from efficiently and effectively disseminating fraud-related information.

Future FPC Fraud Work Group bulletins will explore opportunities for improvements in greater depth as well as a deep dive into a variety of other specific topics. Reducing faster payments fraud to consistently low levels will require shared effort and contribution from participants throughout the ecosystem. These bulletins will continue to lay the groundwork for successful industry-wide efforts to prevent, detect, and mitigate faster payments fraud.

Call to action: Together, we can reduce faster payments fraud to consistently low levels with actions such as the following:

- Collaborate to develop and adopt common fraud prevention processes and technology.
- Improve information sharing practices such as sharing the FPC Fraud Work Group bulletins.
- Participate in industry-wide efforts to prevent, detect, and mitigate faster payments fraud.

Acknowledgements

Fraud Work Group

Thank you to the members of the FPC Fraud Work Group, sponsored by Verafin, who contributed to this bulletin.

FWG Leadership

Lee Kyriacou (Work Group Chair), The Clearing House
Amanda Compton (Work Group Vice Chair), Arvest Bank

FWG Contributors

Neil Kumar, Alloya Corporate FCU
Steve Mott, BetterBuyDesign
Chris Garcia, Commerce Bank
Michael Timoney, Federal Reserve Bank
Ajay Guru, Guidehouse
Scott Anchin, Independent Community Bankers of America
Rene Perez, Jack Henry & Associates
Kalpashree Gupta, KNEKXT Group LLC
Andrew Gomez, Lipis Advisors
Ashley Weinke, Lumin Digital
Liam Cooney, Mastercard International
James Watts, Mitek Systems, Inc.
Carla Sanchez-Adams, National Consumer Law Center
Gail Hillebrand, National Consumers League
Deborah Baxley, PayGility Advisors LLC
David True, PayGility Advisors LLC
Ryan Dutton, SHAZAM
Malinda Rickel, The Banker's Bank - OK
Chris Selmi, WesPay

About the Fraud Work Group

The FPC Fraud Work Group's mission is to collaborate with payments stakeholders to identify, prevent, and mitigate faster payments fraud.

About the U.S. Faster Payments Council

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. By design, the FPC encourages a diverse range of perspectives and is open to all stakeholders in the U.S. payment system. Guided by principles of fairness, inclusiveness, flexibility, and transparency, the FPC uses collaborative, problem-solving approaches to resolve the issues that are inhibiting broad faster payments adoption in this country.

References

[1] Disclaimer: The contents of this bulletin are for educational purposes only and not intended to be legal advice and represents only the views of the Faster Payments Council.

[2] Faster Payments Council. (2022, July). *Examining Faster Payments Fraud Trends.* https://fasterpaymentscouncil.org/userfiles/2080/FraudInfoSharingWP.pdf.

[3] Faster Payments Council. (2022, March). *2021 Faster Payments Fraud Survey and Report.* https://fasterpaymentscouncil.org/blog/8621/2021-Faster-Payments-Fraud-Survey-and-Report.

[4] Faster Payments Council. (2022, July). *Faster Payments and Financial Inclusion.* https://fasterpaymentscouncil.org/userfiles/2080/files/Financial%20Inclusion%20White%20Paper_7-29-2022_Final.pdf.

[5] ACI Worldwide. (2022, November 15). *Growth in APP Scams Expected To Double by 2026 – Report by ACI Worldwide and GlobalData.* https://investor.aciworldwide.com/news-releases/news-release-details/growth-app-scams-expected-double-2026-report-aci-worldwide-and.

[6] AFP. (2023). *2023 AFP Payments Fraud and Control Survey.* https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud.

[7] The Federal Reserve. (n.d.). *FraudClassifier℠ Model.* Retrieved January 19, 2024, from https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/.

[8] The Federal Reservce. (2023, September 15). *Federal Reserve System announces industry-recommended scams definition.* https://www.frbservices.org/news/fed360/issues/091523/industry-perspective-scams-definition-announcement.

[9] In this case "liability" refers to the institution being liable for defaming a suspected fraudster in the case that the suspicion was wrong.