2021 Faster Payments Fraud Survey and Report

Table of Contents

Introduction

Overseen by the U.S. Faster Payments Council (FPC), the Fraud Information Sharing Work Group (FISWG) is focused on providing valuable insights to users and providers of faster payments with respect to fraud prevention, fraud themes and trends, and improving the safety and security as new solutions and networks are launched. In July 2020 the FISWG published the *Examining Faster Payments Fraud Prevention* white paper, examining the current fraud themes and trends, and approaches for mitigating these risks in a faster payments environment, receiving a warm welcome by practitioners and financial organizations alike. In response, the FISWG was called upon to provide more details on actual types of fraud occurring in conjunction with faster payments, how the fraud is being tracked, preventative tools implemented to protect against fraud, etc.

The FISWG met this call to action by conducting its inaugural Faster Payments Fraud survey in August 2021 with the objective of obtaining both quantitative and qualitative data from members of the FPC. The results of this survey were later synthesized to identify commonalities, outliers, and similar findings of interest, and consolidated in this first edition of the FISWG ***Faster Payments Fraud Survey and Report***. In addition to consolidating the survey results, this report provides insight in comparison to non-U.S. geographies, providing a global context of faster payments and fraud.

The intent is for this survey to be the first of many, with subsequent surveys issued periodically, potentially every two to three years, depending on interest from the industry. Future surveys will incorporate learnings from each preceding survey; we welcome your feedback in the continued evolution of this survey and report. The following report begins with an international perspective, then shifts focus to the United States and the 2021 report. We hope you find this document insightful and valuable.

Research

Overview

We conducted domestic and international research to identify what fraud trends emerged after launching faster payments, statistics on fraud (if available), and what mitigation techniques were employed. These insights served to inform our survey design and to understand lessons learned from other faster payment system deployments globally.

The Faster Payments Council has compiled this research using publicly available reports, statements, and similar documents, and does not assume responsibility for their accuracy. We encourage readers to share any additional information or corrections on faster payment fraud trends and mitigation techniques. Please email the FPC at memberservices@fasterpaymentscouncil.org with "FPC Fraud Information Sharing Survey" in the subject line. Additions and corrections will be incorporated into subsequent editions of this white paper as we conduct future surveys.

The FISWG team reviewed faster payments from the following geographies:

Country	Faster Payment System	Launch Year	2020 Payment Value	2020 Payment Volume (Millions)	Fraud Stats (If available)
Brazil	PIX	2020	24.2B BRL	(launched Nov 2020)	
France	CORE IP	2017	Unconfirmed	69.5	~16,000 cases amounting to 150M EUR (bank transfer only, 2019)
India[1]	IMPS	2010	29.41T INR	3,280	
India	UPI	2016	41.04T INR	22,330	
Japan	ZENGIN	1973 (24/7 in 2018)	26,574 B JPY	1,657	APP Fraud 2019: ~17,500 cases, ~ 30B JPY
Mexico	SPEI	2004 (24/7 in 2016)	739B MXN	Unconfirmed	
Nigeria[2]	NIP	2011	11.8B NGN[3]	655.7	NIBSS Fraud in the Nigerian Financial Services
Philippines	InstaPay	2018	463.4B PHP	87	

[1] Retail Payments Statistics On NPCI Platforms, NPCI, July 2021
[2] Fraud in the Nigerian Financial Services, NIBSS, 2020
[3] NIBSS Insight (3rd Edition): Instant Payments - 2020 Annual Statistics, NIBSS, April 2021

Country	Faster Payment System	Launch Year	2020 Payment Value	2020 Payment Volume (Millions)	Fraud Stats (If available)
Poland	BLIK	2017	Unconfirmed	412	
Singapore[4]	FAST	2014	1,434 SGD (Avg.)	147	200M SGD[5]
South Africa[6]	RTC	2006	600B ZAR	49	2B ZAR[7] ([10]1M USD)
Switzerland	SIC	1987	45,266B CHF	728	8.9M, 10.041 bps 2020 (est.)
UK[8]	FPS	2008	2.1T GBP	2,900	34K+ cases valued 145M GBP 1H2018 208M GBP APP fraud 1H2019 (full 2019: 600M USD)
US	Zelle	2017	307B USD	1,200	

Fraud Trends

Each market analyzed experienced an emergence of various scams centered around Authorized Push Payment (APP) fraud. These scams typically included:

Variations of authorized push payments fraud and scams[9]

- Romance scams
- Social engineering
- Phishing
- Vishing

[4] 2020 Retail Payment Statistics for Selected Payment Systems and Industries in Singapore , Monetary Authority Of Singapore, 2020

[5] MAS taskforce to make clear the liability held by consumers, financial firms in e-payment scams, The Business Times, July 2021

[6] SA banks are 'forced' to charge more for instant payments – but their prices vary wildly, Business Insider South Africa, May 2021

[7] Internal payments fraud on the rise in South Africa and costing businesses, apantech, July 2021

[8] Faster Payments System Statistics, pay.uk, June 2021

[9] Faster Payments Council. (2020, July). *Examining Faster Payments Fraud Prevention*. https://fasterpaymentscouncil.org/userfiles/2080/FraudInfoSharingWP.pdf

[10] Techpoint Africa. (2021, February 22). *In 2020, Nigeria lost N5b to fraud in 9 months: what you need to watch out for.* https://techpoint.africa/2021/02/22/nigeria-lost-5b-fraud-2020/

Faster Payment Fraud Vectors

- Mule activity
- Malware
- Remote Access Tools (RATS)
- SIM cloning
- Withdrawal fraud[10]

One outlier was a major fraud perpetrated by an organized crime ring against three Mexican banks in April 2018. Fraudsters stole an estimated USD$18-20 million in unauthorized SPEI transfers[11].

Mitigation Techniques

Mitigation techniques fall into seven categories: 1) bank/provider processes, 2) bank/provider tools and technology, 3) shared information among industry players, 4) public awareness, 5) delayed processing, 6) attack testing, and 7) regulation and oversight.

1. Bank/Provider Processes

- Sending and receiving financial institutions typically employ real-time, active fraud detection solutions that identify and interrupt suspicious transactions. Consistent with other payment channels, OFAC screening and BSA monitoring play critical roles in identifying illegal activity in faster payments. If suspicious activity is detected on an account, instituting transaction limits, temporarily rejecting faster payments, or closing an account can help prevent other fraud attempts until an investigation is complete. Financial institutions work to balance legitimate customer needs with fraud protection.
- **Brazil** – A rash of "Lightning kidnappings," in which people are grabbed off the streets and held until they make a cash transfer for ransom, have resulted in the central bank imposing transaction limits for the Pix system. There is now a $200 limit during the hours of 8 pm to 6 am, a minimum wait time to increase transfer limits, and the ability to tailor transaction limits for day and night.12
- **Singapore** – The advent of contact tracing apps has started a new conversation for other companies that will create faulty apps meant to be deployed to bait fraudsters in which their geolocation is identified with law enforcement to follow.

[11] Wired. (2019, March). *How Hackers Pulled Off a $20 Million Mexican Bank Heist*. https://www.wired.com/story/mexico-bank-hack/

[12] PYMNTS.com. (2021, September 6). *Brazil Limits Pix Payments Amid Kidnapping Spree*. https://www.pymnts.com/news/international/2021/brazil-limits-pix-payments-amid-kidnapping-spree/

2. Bank/Provider Tools and Technology

The FPC's 2020 white paper, *Examining Faster Payments Fraud Prevention*, outlined several technologies and tools being used in the market. These included tools for **login authentication** such as behavioral biometrics and multi-factor authentication, **transaction monitoring** such as AI/machine learning and text alerts, **account tokenization and validation** services, and **basic system security controls**. During our research, we found that providers mention the use of the following tools and technologies:

- **Rules**
  - **US –** Providers are using rules engines based on known key words (e.g., "puppy") and other custom filters based on observed fraud patterns. Providers are also checking transactions against lists of blocked or high-risk recipients, known money mules, and known fraud addresses.
- **Account tokenization and validation**
  - Confirmation of Payee (CoP) is a common validation to help a sender confirm the intended recipient of a payment.
  - **India** – Similar to the use of email addresses and mobile numbers as account aliases in Zelle and other payment services, Virtual Private Address (VPA) is a feature of India's UPI system which replaces bank account details with an alias that resembles an email address. Examples include: 'geooorge@hdfcbank,' 'anjeliene25@upi', and '123456789@ybl.
  - **Sweden** – BankID authenticates the sender. The faster payments app, Swish, redirects the sender to a separate app – BankID – to authenticate with biometrics or passwords. This prevents account takeover and unauthorized payments from stolen devices.[13]
  - **South Korea** – Mentions the use of escrow services.[14]
- **Machine learning**
  - **UK** – After experiencing a fraud spike following the introduction of FPS, UK banks implemented real-time machine learning fraud detection, enabling them to block suspicious payments.[15]
- **Security controls**
  - **EU** – Multi-factor authentication is required by PSD2 in the SEPA.
  - **India** – In 2019, a group of researchers from University of Michigan conducted a detailed analysis of security vulnerabilities among India's top seven UPI payment apps and found vulnerabilities including unauthorized registration and unauthorized transactions with or without debit card/bank account numbers. The group reported its findings to the National Payments Corporation of India (NPCI) so that subsequent versions of the UPI protocol could address these vulnerabilities.[16]

[13] Swedbank. (n.d.). *How to get Swish*. Retrieved January 10, 2022 from https://www.swedbank.se/en/private/digital-and-telephone-services/the-private-app/swish.html

[14] Investopedia. (n.d.). *Definition of Escrow*. Retrieved January 13, 2022 from https://www.investopedia.com/terms/e/escrow.asp.

[15] FICO. (2018). *Fraud in a World of Real-Time Payments*. https://www.fico.com/sites/default/files/2018-06/FICO_Fraud_in_the_World_of_Real-Time_Payments_4543WP_EN.pdf

[16] University of Michigan. (2019). *Security Analysis of Unified Payments Interface and Payment Apps in India*. https://www.usenix.org/system/files/sec20summer_kumar_prepub.pdf

- **South Africa** – Reported that it was working to build new security systems to prevent hacking of databases.

3. Shared Information Among Industry Players

Various entities around the world have established registries and enforced rules requiring ecosystem players to share their statistics on fraud, as follows:

- **Australia** – Banks are obliged to inform the NPPA if they suspect a fraudulent PayID is registered. PayID also checks registrations so that the name registered matches the name on the account.
- **Denmark** – Banks are required to adhere to the Framework Agreement on Participation in the Core Infrastructure (signed with Mastercard/Nets) regarding information sharing and fraud resolution. PSPs in Denmark must report fraud data because of payer manipulation (APP).
- **EU/SEPA** – PSD2 requires that fraud be reported.
- **India** – The Reserve Bank of India established the Central Payment Fraud Registry in 2019.[17] Digital payments service providers will now have to report payment frauds to the registry,[18] and payment system participants are provided access to the data for near-real time fraud monitoring.
- **Nigeria** – Industry data is collected through the Nigeria Inter-Bank Settlement System Plc (NIBSS).
- **Nordics** – Regional portal (Nordic Financial Cert) is used to access and share fraud-related information. Member banks can share and report fraud using account numbers and IP addresses.
- **UK** – Cifas,[19] a fraud prevention community, is the UK's largest cross-sector fraud sharing organization.
- **UK** – Vocalink has a system that traces the movement of laundered or stolen funds.
- **US** – The Fed Payments Improvement community formed the Secure Payments Task Force[20] in 2015. This group wrapped up its work in 2018.

There are a couple of examples of a different kind of information sharing: informing the recipient or beneficiary party of the sending party's internal fraud score, as noted:

- **France** – STET scores transactions using bank account and card-related data, historical data, bank account data, transaction value, date and place of birth, timestamp, IP address, and device ID. This is unique in that both card and account data are used. Banks that have signed up for this service receive these scores.

---

[17] Trak.In. (2019, August 8). *Govt. Aims To Stop Digital Payment Frauds By Central Payment Fraud Registry: How Will It Work?* https://trak.in/tags/business/2019/08/08/govt-aims-to-stop-digital-payment-frauds-by-central-payment-fraud-registry-how-will-it-work/

[18] TECHCiRCLE. (2019, August 8). *RBI to set up central fraud registry for digital payments*. https://www.techcircle.in/2019/08/08/rbi-to-set-up-central-fraud-registry-for-digital-payments

[19] Cifas. (n.d.). Retrieved January 10, 2022 from https://www.cifas.org.uk/

[20] Secure Payments Task Force. (n.d.). *Information Sharing Data Sources*. Retrieved January 10, 2022 from https://securepaymentstaskforce.org/information-sharing-resource-category/data-sources/

- **Netherlands** – Utilizing empty ISO 20022 fields to share the internal fraud score from sending party to receiving party. This enables the receiving party to better judge borderline cases where the information it has may be insufficient to flag a transaction as fraudulent.

4. Public Awareness

- **India** – Since 2016, the Reserve Bank of India has been running social media campaigns about fraud and security threats including UPI: "RBI Kehta Hai" (Central bank says). They recently augmented their approach with a song by the popular rapper Viruss.[21] Additionally, PhonePe, one of India's top payment apps, launched a security awareness campaign in late 2020. The campaign, consisting of a number of short videos, uses the ten faces of a demonic king, Ravana, to represent the ten new faces of evil (i.e..,. payment fraud).[22]
- **UK** – Faster Payments has a campaign called "Take Five to Fight Fraud"[23] which advises people to 1) never disclose security details such as PINs, 2) do not assume email requests or callers are genuine, 3) do not be rushed, 4) listen to your instincts, and 5) stay in control.

5. Delayed Processing

Financial institutions around the globe have implemented tactical, delayed processing to slow down suspicious transactions and perform investigations. Faster payments networks have rules outlining the timeframes in which a payment must be conducted but offer exception processing options for fraudulent activity.

- **Mexico -** Banks enacted contingency plans, moving to an alternate – and slower – method of processing payments.
- **Switzerland -** In some cases, the payment sender's bank may withhold the payment to check it for fraud risk .
- **South Korea** – Concerns about fraud led to the 2015 introduction of a "delayed transfer system" .

6. Attack Testing

- **Singapore** – Conducts offensive simulation exercises: Adversarial Attack Simulation Exercises (AASE), often referred to as Red Team (RT) exercises, to enhance the resilience of a financial institution. The objective is to prevent, detect and respond to fraud. The country also has a Penetration Testing guide.

---

[21] BusinessToday.in. (2021). *RBI ropes in Punjabi rapper for awareness campaign on cyber fraud*. https://www.businesstoday.in/latest/economy-politics/story/rbi-ropes-in-punjabi-rapper-for-awareness-campaign-on-cyber-fraud-289002-2021-02-22

[22] Adgully. (2020, October 28). *PhonePe launches Fraud Awareness Campaign*. https://www.adgully.com/phonepe-launches-fraud-awareness-campaign-97791.html

[23] Faster Payments. (n.d.). *Take Five to Fight Fraud*. Retrieved January 10, 2022 from https://www.fasterpayments.org.uk/take-five-fight-fraud

- **South Africa** – Task bots that can extract and file data from users based on specific commands which will prompt the authorities on where this individual is located.

7. Regulation and Oversight

Some countries provide authority to government agencies or third-party independent alternative dispute resolution groups to help mediate APP fraud scam victims in events where complaints are unresolved between the victims and financial institution.

- **India** – National Payments Corporation of India (NPCI) offers a Dispute Redressal Mechanism in events where complaints are not resolved by Third Party Application Providers or the Payment Service Provider.[24]
- **Singapore** – Code of Consumer Banking Practice[25] details a Dispute Resolution Process where complaints can be escalated to an independent third-party, The Financial Industry Disputes Resolution Centre Ltd.
- **UK** – The Financial Ombudsman Service (FOS) in the United Kingdom assists victims as an informal and free option to the courts.[26]

There are increasing calls for improved consumer protection:

- **Japan** – Laws exist regarding information sharing, reporting, consumer protection, etc.
- **UK** – Due to the growth and innovation of interbank payments, the UK's Payment Systems Regulator (PSR) issued a call for views regarding the expansion of consumer protection.[27]
- **US** – In June 2021, The Consumer Financial Protection Bureau (CFPB) issued a set of FAQs clarifying that unauthorized electronic fund transfers are all subject to Regulation E. This means that if a consumer is deceived into sharing account access information, the bank is liable for reimbursing the consumer's loss, even if it appears the consumer was negligent.[28]

Various central banks and legislature have enacted guidance or regulations governing payments:

- **Nigeria** – Nigeria Inter-Bank Settlement System Plc. (NIBSS) encourages financial institutions to employ sensitization, technology investment, risk management, effective governance, and industry-wide collaboration.[29]
- Anti-money laundering legislation requires accountable institutions to ensure that proper documentation is provided by a party prior to opening a bank account to prevent a party from

[24] NPCI. (n.d.). *Dispute Redressal Mechanism*. Retrieved January 10, 2022 from https://www.npci.org.in/what-we-do/upi/dispute-redressal-mechanism

[25] Association of Banks in Singapore. (2017, November). *Code of Consumer Banking Practice*. https://www.abs.org.sg/docs/library/cocbp_nov2017.pdf

[26] Financial Ombudsman Service. (n.d.). Retrieved January 10, 2002 from https://www.financial-ombudsman.org.uk/

[27] Payment System Regulator. (2021, February). *Consumer Protection in Interbank Payments: Call for Views*. https://www.psr.org.uk/media/5ukcrrap/psr_cp21-4_consumer_protection_call_for_views_feb_2021.pdf

[28] CFPB. (2021, June). *Electronic Fund Transfers FAQs*. https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/

[29] NIBSS. (2020). *Fraud in the Nigerian Financial Services*. https://nibss-plc.com.ng/media/PDFs/post/NIBSS%20Insights%20Fraud.pdf

being able to open a bank account in another party's name. These laws also require Institutions to report suspicious payment activity to a central agency and some allow for institutions to conduct information sharing.

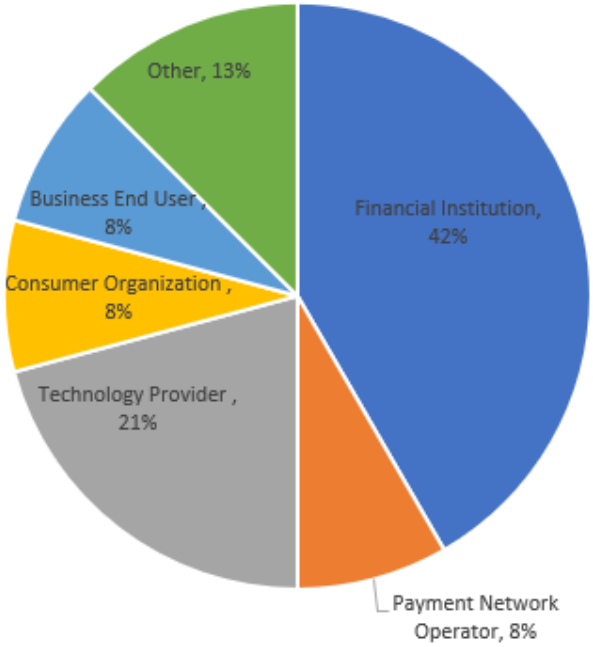
- **Australia** – Anti-Money Laundering and Counter-Terrorism Financing Act 2006.
- **Brazil** – Law No. 9,613/1998 and Law No. 13,974/2020.
- **EU** – Directive 2015/847 and Directive 2018/843.
- **India** – Prevention of Money Laundering Act, 2002.
- **South Africa** – Financial Intelligence Centre Act, 38 of 2001.
- **US** – Bank Secrecy Act, (BSA), Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.

Fraud Survey Results and Findings

Turning our attention from an international perspective, we now focus on the domestic-U.S. market through the review and analysis of the inaugural Fraud Information Survey conducted by the FISWG in October 2021. This survey was sent to members of the U.S. Faster Payments Council to establish a baseline understanding of fraud themes, trends, mitigation approaches, and concerns while also creating a foundation for future surveys to be built upon and leveraged for further improvement. Each new year introduces new payment solutions as well as tactics by fraudsters and bad actors to thwart the systems' controls and prey upon potential victims who leverage said solutions. In response, this survey has promise to periodically obtain an updated temperate of the fraud being perpetrated with respect to faster payments systems within the United States.

The survey consisted of 26 questions covering a variety of topics including use of faster payments, fraud tracking, fraud prevention systems/strategies and future expectations. The questions had multiple response types (e.g., multiple choice or rankings). Most questions allowed comments for additional context. The results were synthesized to identify commonalities, outliers, and interesting data points. For this inaugural survey, we received a total of 24 responses which is important for two reasons: 1) the results of the sample size do not statistically represent the population of FPC members and thus they are not generalizable, and 2) a strong opportunity exists for future FISWG efforts to obtain a higher response rate through increased socialization and potential formatting changes.

Survey Respondents



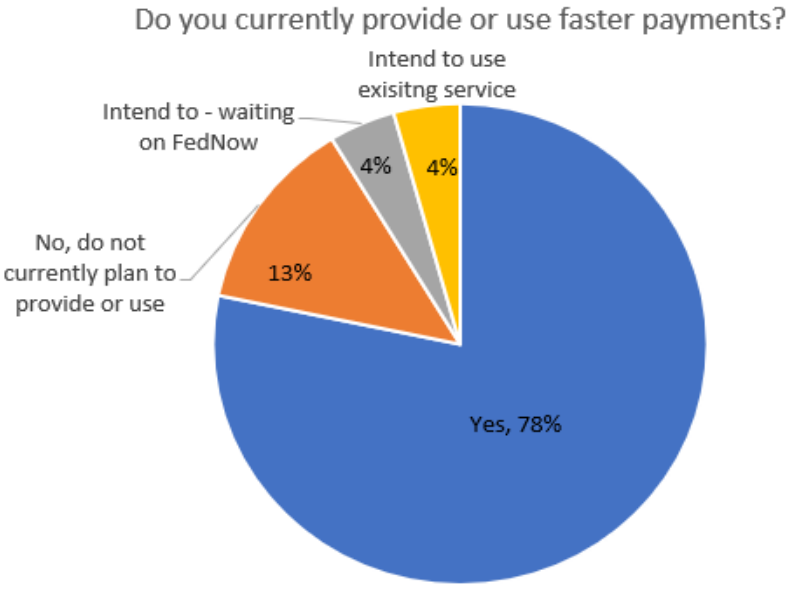
We identified the following themes from the survey responses:

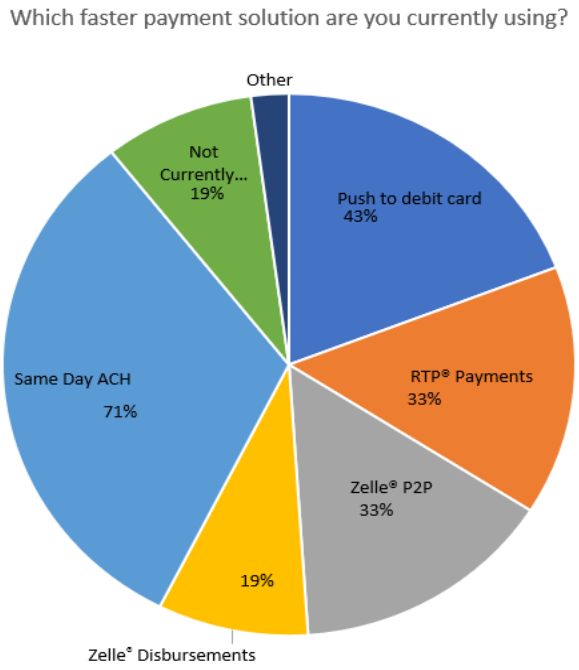
1. Fraud tracking mirrors faster payments adoption but is outpacing fraud prevention.
2. Fraudsters are employing a multitude of strategies and it is incumbent upon organizations to keep pace with equally varied controls and mitigation techniques.
    a. Multiple approaches by both good and bad actors
    b. Data sharing
    c. Future fraud tools
3. Humans continue to be a weak point in the payment ecosystem with account takeover and social engineering being common themes of fraud.
4. Half of respondents are experiencing fraud while half are not.
5. About half the respondents have adopted new operational processes or policies unique to faster payments

Fraud tracking mirrors faster payments adoption but is outpacing fraud prevention

Out of the 24 survey respondents, 18 (75%) are currently providing or using faster payments as defined by the FPC with 2 (8%) planning to offer faster payments,[30] encompassing most survey respondents at 83%. This large adoption rate is encouraging given the premise of the FPC to promote the growth of faster payments across America. Equally encouraging is that 100% of those offering faster payments today who have fraud reporting currently in place, most (80%) tracked both unauthorized and authorized fraud. These statistics are reassuring to know that a balance exists between organizations utilizing faster payments and tracking fraud; however, fraud prevention has fallen short as evidenced in the survey responses.

[30] Payments Innovation Alliance, U.S. Faster Payments Council. (2021). *Faster Payments Playbook*. https://fasterpaymentsplaybook.org/





Examining questions 15 and 16, less than half of respondents (48%) have adopted new technology controls unique to faster payments in addition to those employed in traditional payment methods, and the same percentage of respondents (48%) have adopted new operational processes or policies unique to faster payments use cases in addition to those employed in traditional payment methods, respectively. It is unknown what the overlap is between these two populations; meaning, if respondents have adopted new technology controls only, operational controls only, or both. Many respondents did elaborate as to their reasoning, as follows:

- Technology Controls:
  - "We have added additional authentication technologies to better authenticate the user on the device. We offer the ability to restrict the IP of the user who accesses a security code to the same IP as that of the user who enters it (to stop ATO)"
  - "Real time decisioning with machine learning scores are a must combined with timely and contextualized primary and 3rd party intelligence and behavioural profiling."
- Operational Processes or Policies:
  - "RTP rules require strong authentication & fraud prevention processes not required for other payment system rules. RTP requires FI reporting of all unauthorized payments. Reported unauthorized payments are analyzed to inform future fraud prevention."
  - "Addition of RPA to alerts, triage and cases, and customer SMS/in-App push notifications for greater operational efficiency."

Future iterations of this survey can benefit from obtaining increased insight as to why some users or providers of faster payments have chosen not to implement new technology controls, operational processes, or policies. Furthermore, additional knowledge sharing into which tools have proven to be most effective will allow users and providers of faster payments to have a better understanding as to the optimal model of solutions to complement their risk tolerance while maintaining a specific level of payment friction.

What are your top concerns related to faster payments fraud?
• Operational losses • Real-time alerts • Reputational risk • Recipient risk scoring • Mule accounts • Stronger authentication • Lack of tools • Overhead • Other

Fraudsters are employing a multitude of strategies and it is incumbent upon organizations to keep pace with equally varied controls and mitigation techniques

The fraud prevention role can often feel like a game of "Whack-a-Mole" wherein the organization is constantly discovering new ways fraud has been perpetrated, implementing a solution to eliminate or control for the new fraud event, and the cycle repeats itself in perpetuity. This cycle has not changed with faster payments, but a general perception is that the cycle has accelerated due to the quantity of new solutions entering the market for consumer and business use, and the pervasiveness of fraudsters to capitalize upon nascent solutions to identify their weaknesses for personal benefit. It is to this extent that we examine contributing factors to this perception more closely in three sub-sections as follows.

Multiple approaches by both good and bad actors

As evidenced above with the variety of quoted technology controls and operational processes employed by businesses, technology providers, and financial institutions, multi-faceted approaches are deployed to develop a more robust barrier to bad actors. This varied approach complements the range of techniques by fraudsters as indicated in the open-ended responses to question 14, "Do you see different patterns of fraudulent activity in faster payments than in traditional payment methods?" including:

- "Abuse of immediacy and irrevocability are present. Massive theft/knowledge of PII and theft of OTPs and other step-up authentication also happening. It's faster than before."
- "[W]e are seeing more account takeover and fraud involving digital channels and email"
- "After a data [breach], like T-Mobile, social engineering fraud spikes in our markets."

These new approaches were identified by approximately one-third of survey respondents (32%), with the remaining two-thirds stating that there are no new methods employed by bad actors; to this extent, future iterations of this survey are recommended to explore further if the patterns are simply consistent with traditional payment methods, not occurring, or unknown.

Data sharing

Unfortunately for the payments industry, fraud actors have increased their data sharing and collaboration efforts within their fraud community. Evidence shows that this fraud community is willing to share, teach, and sell information that others can use to commit payments fraud. Financial institutions need to be increasingly aware that fraudsters will identify and exploit any weaknesses they can identify within the system. These weaknesses may allow them to take advantage of the company's own internal policies, practices, and procedures to bypass their existing fraud protections. Additionally, fraudsters share the tools and techniques they have refined, often for a profit, through educational forums where insights and information can be bought and sold.

Regrettably, this type of open partnership among the fraudsters does not always exist within the payment community. There are numerous reasons FIs might not want to share information and many challenges to overcome when we consider data sharing outside our own organizations. Understandably, financial institutions are hesitant to share information across organizations due to risks related to improper sharing, accidental loss, or unauthorized access. Missteps with data could result in negative publicity or financial losses. Additionally, organizations may view their fraud data as an asset in the fight against fraud and may be unwilling to eliminate that competitive advantage by sharing with others. Another big concern for financial institutions is the ability to comply with consumer privacy protections. As these rules are constantly evolving, FIs may be challenged to determine what information they can/cannot share, and when/how they can share. To avoid scrutiny,

organizations may take the safer path and opt not to share at all. The ability to share this type of information typically comes with a financial cost as well; organizations may incur additional expenses for people and technology to collect, ingest or share this type of information. These types of costs may impact some organizations more than others and may eliminate some of the more vulnerable institutions from participating.

Who do you rely on to provide you with latest faster payments scams and fraud information?
• Trade Groups • Internal Resources • Fraud Management Technology Provider • FBI Scams & Safety • Federal Reserve • Core Provider • FTC • News Board • Non-profit • Other

However, if the industry could also partner and potentially share fraud insights, it may be better protected as a whole. Organizations could protect themselves by using this information to identify weaknesses in their policies and procedures. Ultimately the information could be used to bolster existing anti-fraud processes and fraud management strategies to prevent impact from new schemes or shifts across payment types or channels.

The ability to ingest more timely and diverse information can help detect and prevent fraud in this time of faster payments. The lack of timely fraud information exposes the payments industry to potentially greater losses. Similarly, shared fraud information can help financial institutions better distinguish fraud from normal payment activities.

On a positive note, new technologies such as artificial intelligence and machine learning, are being used to overcome these challenges. AI can be used to identify fraud trends, patterns and insights for transactional data and has the potential to share the insights without the sharing of the Personal Identifiable Information (PII). Some existing faster payment networks are requiring participants to report fraudulent transactions; this data is used for the betterment of the network by constantly evolving fraud models to the shifts in fraud.

Future fraud tools

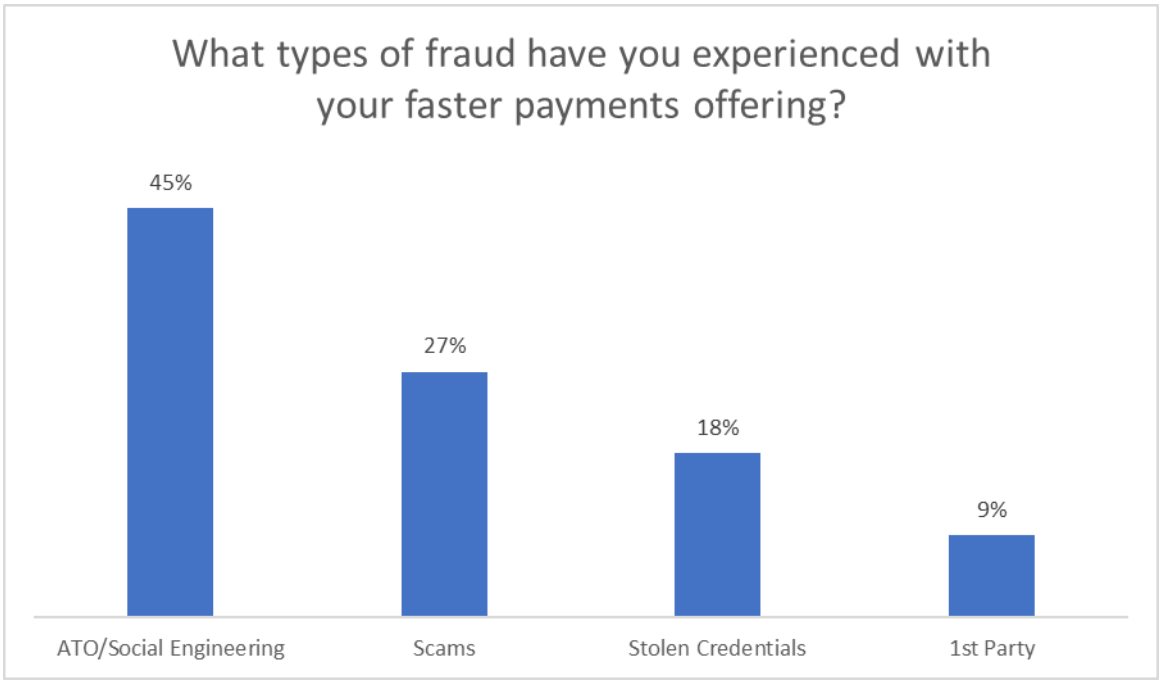
About one-half of the respondents reported that they had adopted new technology controls unique to faster payments in addition to those they employ in traditional payment methods. Of those that have implemented new controls, based on write-in comments, 50% are increasing their use of real-time decisioning and alerting, 40% are relying on artificial intelligence and machine learning, and 30% are improving authentication techniques, such as requiring out-of-band authentication for new payees.

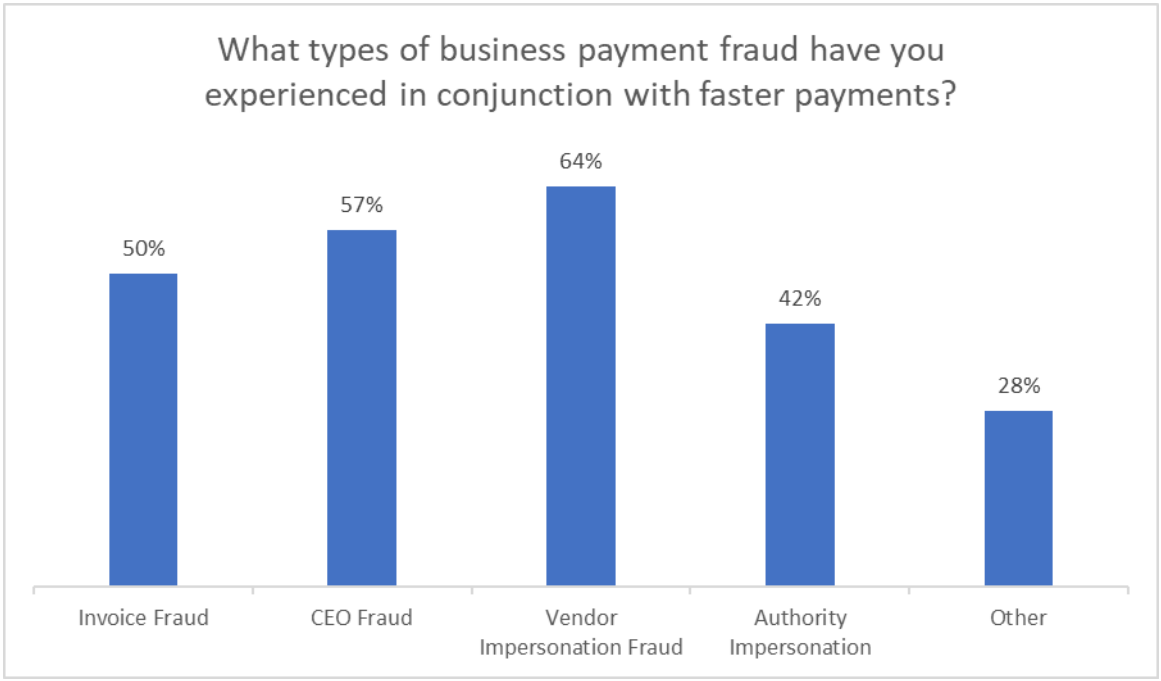
There was interest in additional fraud mitigation techniques based on what other international markets have employed with some success.

- Highest interest was shown for "industry-wide sharing of blocked or high-risk recipients, e.g., known money mules" which was ranked as top choice for more than half the respondents.
- This was followed by "fraud mitigation solution and money mule detection with holistic view of entire market or at the provider level," which was selected as top choice by 30% of respondents.
- The third top choice was "establishment of a consumer protection appeals process for consumers who have been the victims of scams."
- There was comparatively little interest in use of escrow accounts.

Internationally, various mitigation techniques have been adopted to reduce risk with faster payment systems. What is your level of interest in leveraging the following mitigation techniques?
• Industry data sharing • Industry-wide fraud solution • Consumer appeals process • Escrow accounts • Other

Humans continue to be a weak point in the payment ecosystem with account takeover and social engineering being common themes of fraud





Over half the respondents to the survey indicated that they have experienced fraud related to their faster payment offerings. When asked about the kind of fraud experienced most highlight that social engineering tactics were the culprit. Social engineering methods aim to manipulate human behavior to deceive people into providing their credentials through some social interaction (e.g., online, in-person, SMS) by which fraudsters aim to exploit the trust, fear, or curiosity of their target which leads to compromise.

Account takeover (ATO) was highlighted as the method most used by fraudsters in the survey. Account Takeover is a form of identity theft and fraud where a third party successfully gains access to a user's account credentials. While ATO can be the result of a social engineering tactic, fraudsters can also get account credentials through data breaches. The Dark Web is a major source of identity related information and fraudsters can then take this info and combine it with other methods to acquire user credentials. Banks continue to employ mitigation strategies by adding warnings to confirm recipients, as well as multifactor authentication techniques such as SMS with codes which need to be entered for confirmation (e.g., one-time PIN [OTP]). The FISWG published the *Examining Faster Payments Fraud Prevention* whitepaper on faster payments fraud trends which provides additional insight on fraud themes and mitigating strategies to address these methods.

Half of respondents are experiencing fraud while half are not

This is an encouraging number though it does invite further questions as to what those not experiencing fraud are doing differently. Looking at the types of faster payments offered it appears that some are potentially less susceptible to fraud or offer additional controls that help mitigate fraudulent activity. The majority of respondents selected Same Day ACH as at least one of their faster payments solutions. This is predominantly a business offering and has controls built in through access to the online banking platform. It is also generally offered to users experienced with the system and who are familiar with security requirements and best practices.

The next most popular selections were Push to Card followed by Real-Time Payment solutions and Zelle. While available to both consumer and non-consumer, these solutions many times do not include any enhanced due diligence or training prior to use and are generally available by signing up and agreeing to terms and conditions. End users may not fully understand how these payment systems work and are an easier target for scams. The most prevalent type of fraud cited by respondents was Account Takeover and social engineering. These types of scams are neither new nor are they specific to faster payments.

New operational processes or policies implemented by half of respondents

Regarding question 16, "Have you adopted new operational processes or policies unique to faster payments use cases in addition to those you employ in traditional payment methods?" and as

previously mentioned, the responses were evenly split. On the positive side, it is encouraging that 48% have determined that they should implement additional processes or policies to help stop fraud that may be associated with faster payments. It appears they have taken a proactive step to mitigating any potentially new risks. The information does not provide insight if the other 52% already had strong processes in place that would already cover the faster payments or if they determined that the faster payments did not bring additional concerns or risks. With future surveys, this can and should be interrogated more to yield valuable insight.

Closing

Thank you for your interest in the inaugural ***Faster Payments Fraud Survey and Report*** published by the U.S. Faster Payments Council's Fraud Information Sharing Work Group. This document is the first of many and your feedback is valuable to the FISWG; we welcome your insight through active participation in the FISWG and broader engagement with the FPC. Again, we encourage readers to share any additional information or corrections on faster payment fraud trends and mitigation techniques. Please email the FPC at memberservices@fasterpaymentscouncil.org with "FPC Fraud Information Sharing Survey" in the subject line. Additions and corrections will be incorporated into subsequent editions of this white paper as we conduct future surveys.

Contributors

Thank you to the members of the FPC Fraud Information Sharing Work Group who contributed to this white paper.

- Andrew Haskell (Work Group Chair), BNY Mellon
- Deborah Baxley (Work Group Vice Chair), PayGility Advisors LLC

Research contributors:

- Neil Kumar, Alloya Corporate FCU
- Lisa Clapes, Ceridian HCM
- Sarah Clark, Commerce Bank
- Richard Bradfute, James Polk Stone Community Bank
- Andrew Gómez, Lipis Advisors
- Shoaib Shafqat, QCheque
- Kim Barsness, SHAZAM
- Jason Paguandas, Visa

Survey & Report Development contributors:

- Olivia Hilton, ABA
- Meredith Pollack, ABA
- Michael Timoney, Federal Reserve Bank
- Tanya Hughes, Guidehouse
- Alla Ilgelnik, Guidehouse
- Rebecca Kruse, ICBA Bancard
- Malinda Rickel, The Bankers Bank
- Elspeth Bloodgood, ProfitStars/Jack Henry
- Peter Tapling, PTap Advisory
- Jenni Giguere, WesPay

Overall contributors:

- Amanda Compton, Arvest Bank
- Karthik Ravichander, Axletree Solutions
- Martin Reyers, BMO Harris
- Christopher Garcia, Commerce Bank
- Brandon Kelly, FirstBank
- Sriram Iyer, FIS Global
- Jonathan Uzzo, Mastercard
- Jordan Bennett, Nacha
- Vladimir Jovanovic, PSCU
- Ryan Dutton, SHAZAM
- John Venglass, Vesta Corporation