FOCUS NOTE

FRAUD RISKS IN FAST PAYMENTS

PROJECT FAST

FRICTIONLESS • AFFORDABLE • SAFE • TIMELY • TRANSACTIONS

OCTOBER 2023

WORLD BANK GROUP

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE
Payment Systems Development Group

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

CONTENTS

1 SETTING THE CONTEXT

The World Bank has been closely monitoring the development of fast payment systems (FPS) by central banks and private players across the globe.[1] This comprehensive study has resulted in a policy toolkit designed to guide countries and regions on the likely alternatives and models that could assist them in their policy and implementation choices when they embark on their FPS journeys.

Work on the FPS Toolkit is supported by the Bill and Melinda Gates Foundation under Project FASTT (Frictionless Affordable Safe Timely Transactions). The toolkit and other relevant resources of Project FASTT can be found at fastpayments.worldbank.org and consist of the following components:

- The main report *Considerations and Lessons for the Development and Implementation of Fast Payment Systems*
- Case studies of countries that have already implemented fast payments
- A set of short focus notes on specific technical topics related to fast payments

This note is part of the third component of the toolkit and aims to provide input on fraud risks facing FPS. This topic is of relevance given the increase in the occurrence and diversity of fraud and financial crimes linked to digital payments and in particular fast payments.

2 BACKGROUND

Fraud is not unique to fast payments and has always existed in payment systems and, more broadly, in all types of financial services and economic activity. Many end users—both businesses and consumers—are often not sufficiently aware of the types of fraud being perpetrated, making them vulnerable to novel types of fraud. Criminals constantly monitor how new technology and payment systems can be exploited and incorporate this information into their toolkits to attack account holders in a multitude of ways.

The Payment Systems Regulator (PSR) in the United Kingdom reported that a mere 0.1 percent of fast payments in the United Kingdom were fraudulent in 2021. Despite constituting a relatively small percentage of fast payments, this figure is much higher than the 0.03 percent global average for card transactions. Furthermore, the harm that payment fraud inflicts upon consumers and businesses can be significant and necessitates proactive measures by regulators and stakeholders. Safeguarding the integrity and security of FPS is imperative to maintaining trust in the financial ecosystem and ensuring that the threat of fraud does not overshadow the benefits of swift, convenient transactions.

Increased adoption of fast payments has indeed led to an uptick in fraud in some markets. In the United States, Zelle, a mobile-based account-to-account (A2A) alias service, has been significantly affected by fraud cases in recent years. Studies show a 280 percent increase in total fraud value on Zelle between 2020 and 2022, with losses totaling $255 million in 2022.[2] The volume of fraudulent transactions on Zelle has also increased considerably, with nearly 36,000 cases in the period between 2021 and 2022. A considerable amount of this fraud is so-called "authorized" fraud involving scammers who pose as friends or merchants to trick victims into sending money to their accounts. Similarly, in Brazil, the increased adoption of fast payments and the success of Pix have also led to increases in fraud. Recent losses resulting from fraud in the country have been considerable, with total damages estimated at about R$2.5 billion ($500 million) in 2022. Seventy percent of these cases stemmed from operations using Pix. Responses from the Brazilian government have included caps on peer-to-peer transfers during certain hours and enhanced mechanisms for fraud resolution, among others, although fast payment fraud continues to be a persistent challenge.

The United Kingdom has also experienced an alarming surge in fast payment fraud in recent years. Authorized push payment (APP) fraud and remote banking fraud are especially prevalent, amounting to £485.2 million ($629.03 million) and £163.1 million ($211.4 million) in losses, respectively, in 2022. This has led the industry to adopt a multifaceted approach to fraud prevention, which has shown some positive effects, as APP fraud decreased by 17 percent from 2021 to 2022. Total fraud losses still amounted to roughly £1.2 billion ($1.56 billion), however. Fifty-three percent of losses stemmed from either authorized or remote banking fraud, underscoring the ongoing need for continued vigilance and innovative strategies. Moreover, the vast majority of APP fraud in the United Kingdom (95.6 percent of cases and 83.1 percent of loss values) is committed using the Faster Payments System, illustrating how FPS can become a prime target for APP fraud.

One of the key benefits of FPS is that they enable the immediate initiation and receipt of payments 24 hours a day, seven days a week, 365 days a year. However, the speed at which funds become available to the recipient is often what makes fast payments attractive for fraudsters. Over recent years, fraud has "migrated" from batch-based payment systems to FPS for this reason. On the other hand, social engineering techniques, which existed long before the introduction of fast payments, have become easier to carry out, as artificial intelligence is used more and more and fast payments are integrated with other social and e-commerce apps. Moreover, several other key features of fast payments make them attractive for consumers, businesses, and merchants, such as relatively high value limits and payment finality, as outlined in table 1.

TABLE 1 **Key Features of Fast Payments and Relevant Considerations for Fraud**

Key Features*	Indicative Benefits	Fraud Considerations
Posting speed	• Funds are available to the beneficiary in seconds. • Funds are sent to a bank account, not to a prepaid/prefunded instrument that needs to be funded/defunded.	• Strict service-level agreements based on scheme rules mean that payment service providers and FPS operators have little time to run fraud checks (such as anti-money-laundering or countering the financing of terrorism). • Even if fraud is identified, the time to respond is much shorter because the recipient has immediate access to funds and can move them between many accounts (that is, so-called money mules).
24/7/365 availability	• Continuous system availability mimics features of cash. • Increases utility for the sending and receiving parties.	• Fraudsters can work around the clock and at odd hours, especially when bank staff members are not active. For this reason, victims may not be able to check their accounts and report fraudulent activity to the authorities quickly.
Payment finality	• Provides greater security around the payment because it cannot be reversed. • Helps improve cash flow for companies/merchants. • The lack of chargebacks makes fast payments more attractive than cards in the e-commerce or physical point-of-sale environment.	• Money that is fraudulently stolen from an account cannot be easily reversed, as with a card payment (for example, chargebacks). • By the time a transaction is deemed to have been fraudulent, the illegally obtained funds may already be gone. This can make lost funds very hard to recover.
High transaction limits	• Many FPS have relatively high transaction limits that can support a variety of business use cases. • The higher the limit, the greater the number of use cases that can be supported.	• The ability to send a large amount of money in a single transaction can make fast payments very attractive for fraudsters.

*This list of FPS features is not exhaustive.

3 FRAUD TYPOLOGIES IN FAST PAYMENTS

Fraudsters often adapt their techniques to the local market and the technologies available. However, several fraud typologies can be identified regardless of a market's characteristics: unauthorized fraud, authorized fraud, and friendly fraud. The most common targets are individuals and merchants, although more sophisticated criminals also target payment service providers (PSPs) as well as system operators. This section examines the different techniques swindlers use, the three main fraud typologies, and recent trends.

3.1 FRAUD TECHNIQUES

Cyberattacks

Fraudsters attempt to steal, alter, disable, or even destroy data, applications, or other assets through unauthorized access to a network, computer system, or device—generally referred to as cyberattacks.[3] Attackers may use a variety of sophisticated tactics to obtain unauthorized access to data. Cyberattacks usually try to cause data breaches (that is, a security incident in which an unauthorized party gains access to sensitive data or confidential information) and are the first step for criminals looking to initiate unauthorized payments. Scammers manage to obtain an individual's and/or a business's personal information or credentials, which are then used to manipulate the targets or access payment accounts and initiate transactions. Several forms of cyberattacks are detailed below:

- **Advanced persistent threats:** These are targeted and continuous attacks on IT infrastructures in which fraudsters repeatedly, over an extended period, try to access IT infrastructure. Attackers aim to exploit or obtain data, attack processing systems, infiltrate processing systems to change parameters, and so on. They attack financial systems and other infrastructure used in the payment ecosystem, either from banks, processors, payment system operators, or any other system and technology.
- **Malware:** Malware refers to a diverse set of hostile or intrusive software, such as trojans, remote access trojans, spyware, adware, ransomware, and the like.[4] Cybercriminals design malicious software to compromise security functions in computers and mobile phones to steal data, bypass access controls, and cause harm to both electronic devices and installed applications. Within the payment value chain, payment initiation and authentication methods are often the targets of malware attacks. These range from keylogging (that is, using software that tells the recipient which keys are being typed, enabling fraudsters to capture PINs, passwords, and so on) to capturing online banking and/or payment app credentials to man-in-the-middle attacks. Malware usually searches electronic devices for information that can be monetized. In the case of individual customers, this information usually pertains to credentials related to internet and mobile banking.
- **Man-in-the-middle attacks:** In these attacks, imposters secretly intercept and exchange messages and information with two parties who believe they are communicating directly with each other. For example, fraudsters may intercept communications between a customer's device and the banking server, enabling the attackers to alter and

redirect payment messages. Man-in-the-middle attacks may occur in combination with malware, advanced persistent threats, and phishing attacks to enable unauthorized transactions.

- **Phishing:** Phishing is a form of social engineering in which personally identifiable information about either an individual or an organization is obtained through several possible means, such as email and SMS, among others. Phishing attacks are becoming more sophisticated, moving from emails and text messages to other more personal communication channels and targeting a much more specific group of victims—for example, leveraging occasions such as Black Friday in the United States or Lunar New Year in some Asian countries, targeting specific groups of individuals, or crafting phishing attacks to specific companies, such as when new employees join. Phishing is often used in combination with social engineering to conduct authorized fraud.

Social Engineering

Through social engineering, criminals use an end user's personal details that they collected previously (likely through phishing, data breaches, or even publicly available information that the user shared online) to deceive the user into trusting them. The scammer then convinces the victim to make fraudulent transactions or disclose additional information needed to carry out a transaction. The goal of social

BOX 1 SPECIFIC EXAMPLES OF SOCIAL ENGINEERING AND PHISHING IN FPS

- Nearly 18 million Americans were defrauded through scams involving digital wallets and peer-to-peer payment apps such as Zelle in 2020, according to Javelin Strategy & Research. Recent scams involved spoofed calls to users, where the phone call received appears to come from an individual's bank. One example involved phishing and social engineering: A customer got a call from a number he didn't recognize. A woman who said she worked for the customer's local bank was supposedly calling him to alert him of fraud in his account. "They wanted me to verify my identity through a text code. They sent me a text, and then I read the six numbers back," said the customer. That was all it took for the imposters to create a Zelle account in his name and gain access to both his checking and his savings accounts—all within hours of their phone call. The scammers had tricked this customer into providing them with the code that the bank had sent him to confirm his identity.
- Brazil's highly successful payment system Pix has also been used by fraudsters employing social engineering techniques to conduct APP fraud. Hoaxers gain the victim's trust by pretending to be a friend, a business, or an official and convince the victim to send them money via Pix. In one example, scammers developed falsified payment QR codes, which were attached to fake invoices and bills sent via email to clients. Scammers knew that using the QR code would be tempting to consumers because paying via QR code could lead to a 5 percent discount. Fraudsters intercept emails sent to consumers by billers, such as phone and internet companies, edit the information, and resend the bills containing a fake QR code that directs payments to the imposter. Employing another popular fraud method, criminals create accounts with digital banks under the names of fake companies that resemble real companies, such as "Gooogle." The scammers then reach out to other businesses and ask that the accounts payable team update payment information to the scammers' Pix account.
- In India, too, social engineering schemes developed around the Unified Payments Interface (UPI) have become increasingly common. Payment fraud as a percentage of total digital payments escalated from 0.008 basis points in 2019–20 to 0.0089 basis points in 2021–22. Scammers often assume the guise of trusted customer service representatives from reputable banks. Through manipulative tactics, these malicious actors persuade unsuspecting customers to engage in the completion or the updating of their online electronic know-your-customer information, ostensibly to ensure the continued activity of their accounts. Through this manner, criminals gain access to sensitive and confidential information, allowing them to orchestrate illicit transactions, often exploiting OTPs shared during their fraudulent interactions. These perpetrators may go further, soliciting personal information such as Aadhaar numbers, biometric data, or additional OTPs under the pretext of resolving purported issues.

engineering is to manipulate individuals to compromise accounts, not to hack electronic devices such as computers and mobile phones.

Fraudsters have increasingly used social engineering to solicit users' one-time passwords (OTPs) to authorize transactions or register for a payment application, mobile banking application, or general authenticator application. Scammers may also trick victims into believing that relatives or friends are in distress and ask for financial help or solicit donations for some topical social cause.

Impersonation Techniques

Scammers may impersonate government officials, bank staff members, business employees, relatives, and any other party that helps them persuade victims to provide relevant information or carry out transactions. Many types of APP fraud, described in detail in the next section, involve impersonation. Imposters may also use current economic and societal circumstances to their advantage, such as a natural disaster or the COVID-19 pandemic, or target specific demographic groups, particularly young people and the elderly.

Hoaxers in Japan, for example, have been utilizing impersonation techniques for many years to conduct authorized fraud. Because Japan's elderly population is large, these types of scams are very common. In the so-called "it's me, it's me" scam, fraudsters impersonate the elderly's children or grandchildren over the phone and ask urgently for money transfers. Scammers also impersonate victims to obtain information from their banks, often using data previously obtained through phishing, after which they can change the victim's account settings or swap the user's mobile number to a SIM card controlled by the fraudster to receive OTPs.

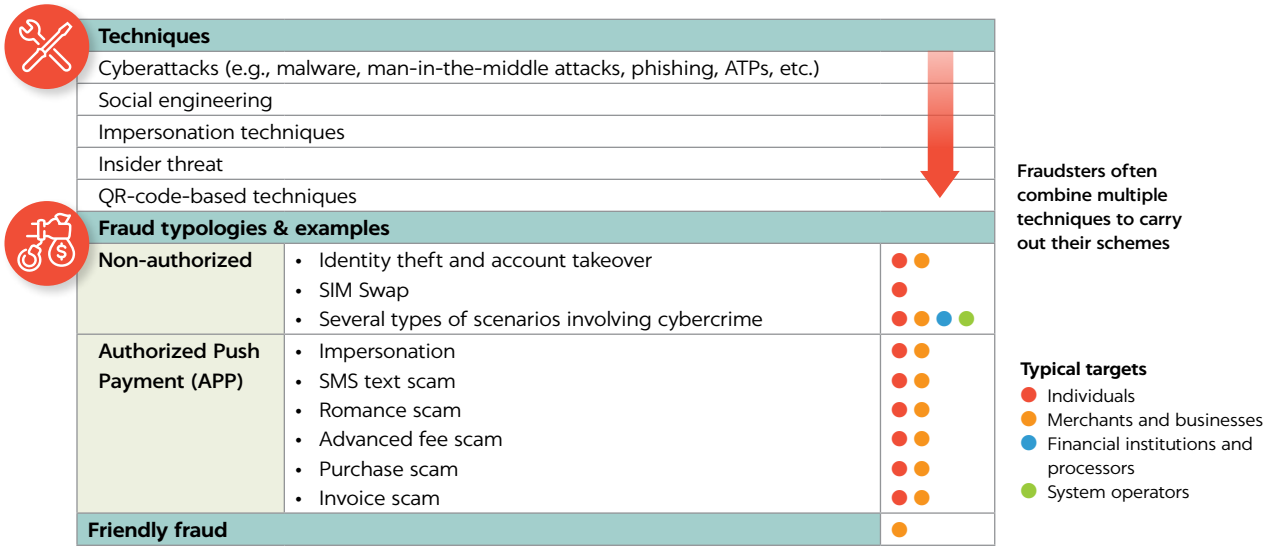
QR Code–Based Fraud Techniques

QR codes provide an easy-to-scan image that redirects the scanner to a database that contains information related to the QR code, often the beneficiary's payment information. Scammers may manipulate QR codes to obtain users' information (known as "quishing"), redirect users to fake websites, make users download files and/or applications infected with malware, or replace the original payment information with the fraudster's payment information. At the point of sale, this can occur by replacing an existing QR code with a phony QR code that is designed to look like the merchant's QR code. Several payments may be initiated before the merchant and/or customer realizes the QR code is providing fraudulent payment information. These techniques are becoming more prevalent as QR code–based payments increase in relevance, particularly for consumer-to-business payments.

3.2 COMMON FRAUD TYPOLOGIES

The techniques described in the previous section ultimately result in different types of payment fraud. Developing a framework for understanding the different types of fraud is useful because the different types often require different solutions. For example, multifactor authentication (MFA) techniques can effectively combat unauthorized fraud, but they do not help prevent authorized fraud. Figure 1 provides an overview of the different techniques commonly

FIGURE 1 **Common Fraud Scenarios in Fast Payments, Fraud Techniques, and Enablers**



Source: World Bank

used to perpetrate fraud, examples of authorized and unauthorized fraud, and the typical targets of each type.

Unauthorized Fraud

Unauthorized fraud occurs when the payer's account is taken over by a fraudster who then makes unauthorized payments from the victim's accounts. Relevant techniques include the use of malware, phishing, or even social engineering to gain access to the account. Common types of unauthorized fraud include identity theft, SIM swap, and cybercrime. For example, a victim may receive a text message from a scammer impersonating a government official working on pandemic support, including disbursements of stimulus. The imposter asks the victim to provide personal information to verify the individual (and, fittingly, avoid duplication of aid disbursement). The scammer uses this information to obtain personal information (date of birth, place of birth, home address, and so on) and can then call the bank and change the victim's account settings (such as the daily limit on money that can be sent from the account). This is possible due to the amount of information that the scammer has and the cheater's ability to convince the bank employee over the phone that the fraudster is the account holder. The hoaxer is now able to initiate a series of transactions—which now have a higher limit because the fraudster increased it—and empty the victim's bank account. Another example involves a scammer infecting a victim's device with malware, providing the attacker with the victim's personal information. The imposter uses this information to transfer funds from the victim's bank account.

SIM swap fraud is a relatively new form of fraud that is on the rise in various markets, such as Colombia, Nigeria, and South Africa. In SIM swapping, a scammer manipulates a telecom employee into believing that the fraudster is a customer and requests to move the phone number to new a SIM card that the scammer controls. This can be done by exploiting the personal data or credentials of the victim obtained through phishing, a data breach, or other means. Any OTP tied to the victim's phone number is instead sent to the fraudster. Assuming that the user's credentials have also been obtained, the scammer can then authorize transactions from the victim's account.

Authorized Push Payment Fraud

APP fraud is different from traditional fraud because the payment itself is not fraudulent—the individual initiating the payment is the account holder who intends to make the payment but under false pretenses. The beneficiary may be pretending to be someone they are not or may have convinced the sender that they intend to help the payer or provide a good or service.

When committing APP fraud, fraudsters often move the funds out of the receiving account quickly, so that the money cannot be returned to the sender once the fraud is realized and reported. Fraudulently received funds are then often sent to "money mules"—individuals who move money on behalf of the imposter, sometimes knowingly, other times unknowingly—and transferred many times before eventually being withdrawn, transferred out of the country, or moved into the cryptocurrency space.

APP fraud often utilizes social engineering, phishing, and/or impersonation. Criminals use social media to approach victims and may copy advertisements for goods and services that never materialize. There are many types of APP

FIGURE 2 Common Mechanics of Identity Theft

THE MECHANICS OF IDENTITY THEFT:

- Through various techniques (social engineering, spyware or malware, mail theft, or even bribery) fraudsters obtains victims information.
- Fraudsters take over bank accounts or access bank services to initial payments/acquire financial products on the victim's behalf.
- Funds will be stolen depending on the fraud type.

Source: World Bank

FIGURE 3 Common SIM Swap Mechanics

THE MECHANICS OF SIM SWAP:

- Fraudsters acquires victims information.
- Fraudsters calls the telco operator and requests a number transfer.
- Telco operator changes the number to the fraudsters SUM.
- The fraudsters bypass two-factor authentication.
- Bank transfer fraud is committed.

Source: World Bank

fraud, but common examples include advance fee scams (pay a small fee now to receive a larger discount on goods or services later), invoice scams (a fake invoice is created for a supplier or biller that may not even exist), romance scams (the scammer pretends to need money to meet the victim in person, deal with an unexpected health issue, or other reason), CEO scams (the purported head of a company writes, asking a colleague to buy gift cards for clients with whom the CEO is about to meet), and so on.

Most regulatory frameworks do not provide legal protections for victims of APP fraud, as they do for victims of unauthorized fraud. However, payment ecosystem stakeholders across the globe are increasingly acknowledging the need for regulatory and/or industry-led actions to protect consumers. Worth highlighting are efforts by the European Union, Japan, and the United Kingdom aimed at preventing users from becoming victims of APP fraud or helping to recover stolen funds. Victims of unauthorized fraud, on the other hand, are typically protected and will recover at least some of the losses.

Friendly Fraud

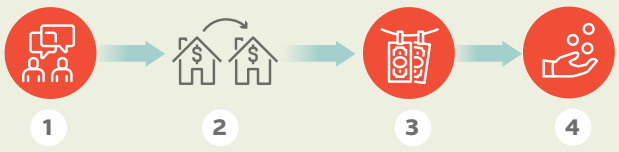
Friendly fraud has traditionally been prevalent in the cards space, whereby the fraudster abuses the chargeback abilities of a card—often a credit card—to reverse legitimate charges. In other words, a consumer buys a good using a card and then calls the bank that issued the card and claims that the good or service was not purchased by them and requests the money be returned. The issuing bank then retrieves the funds back from the merchant's bank (acquiring bank), which in turn takes the money back from the merchant. While friendly fraud is typically associated with card payments, the use of fast payments for online consumer-to-business transactions makes it necessary for merchants and businesses to implement strategies to mitigate risks.

One of the problems with dealing with friendly fraud is that the very protections that shield consumers from unauthorized fraud can be abused. In section 2.1.1, the finality of a payment was listed as one of the key characteristics of fast payments precisely for this reason: they protect merchants from unscrupulous consumers who wrongfully claim that a product or service was not ordered. In some markets, such as the United Kingdom, consumers can request that money be returned regardless of whether the fraud in question was authorized or unauthorized. This means that the possibility exists that some will abuse these protections and perpetrate friendly fraud. It is difficult to prove whether friendly fraud has occurred, so the issuing bank often initiates a chargeback to keep the customer satisfied. Friendly fraud has grown in recent years due to the rise of e-commerce, as this type of fraud is far easier to commit against online merchants than physical retailers. Victims of this type of fraud are businesses and merchants who suffer damages in the form of lost revenue, chargeback penalties, reputational damage, fraud-prevention costs, and the need to hold liquidity to handle potential chargebacks. All of these costs are then added to the prices of goods and services, harming consumers.

FIGURE 4 Common APP Fraud Mechanics

APP FRAUD MECHANICS EXAMINED:

- Fraudster impersonates a trustworthy invidial or organization and contacts the victim (via phone, email, SMS, etc.).
- Fraudster convinces the victim to send money directly to the fraudsters account (an example of authorized fraud).
- When the fraudsters received the funds they will often transfer the money to mule accounts.
- After laundering the money via mule accounts, the fraudster then cashed out the illicitly gotten funds.



Source: World Bank

FIGURE 5 Common Friendly Fraud Mechanics

FRIENDLY FRAUD MECHANICS EXAMINED:

- The fraudster makes a legitimate purchase from an e-commerce site.
- The fraudster contacts their PSP to dispute the charge and claims the charge was fraudulent in order to get a refund.
- The fraudster gets reimbursed and quickly withdraws the funds.

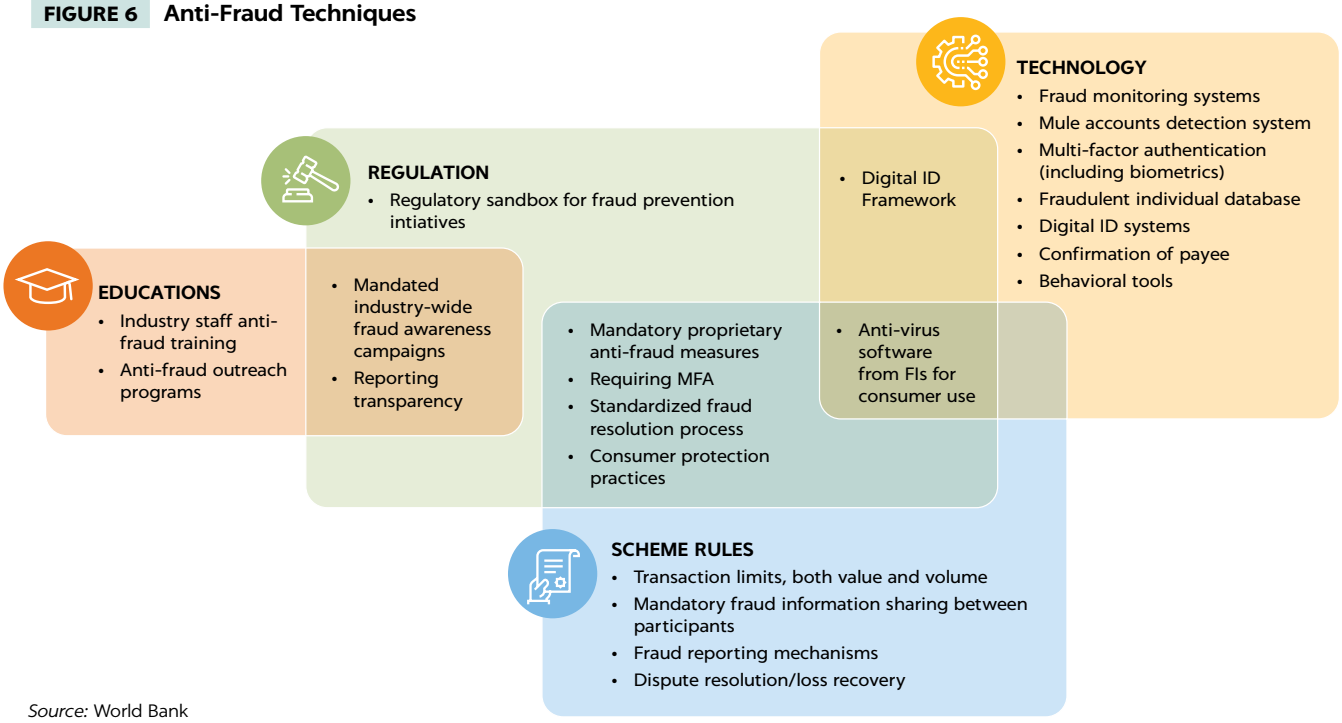
Source: World Bank

4 FRAUD PREVENTION TECHNIQUES

Fraud prevention may often seem to be a never-ending cat-and-mouse game: fraudsters use new techniques to avoid detection or trick victims, while ecosystem actors constantly deploy new software, carry out educational campaigns, or create new regulations to deter fraudulent activity. Fraud prevention is challenging because of the number of potential vulnerabilities at each point in the payment value chain, and mitigation and prevention techniques must be put in place at every level, since scammers seek out weaknesses and then attempt to exploit them. While anti-fraud techniques must work every time along the value chain, criminals often need to succeed only once.

This section details four aspects of fraud-prevention techniques that can be leveraged: scheme rules, technology solutions, regulation, and industry-wide initiatives, such as education. It should be noted that there is considerable overlap between each of these approaches. As figure 6 shows, almost all techniques can be put into two or even

FIGURE 6 **Anti-Fraud Techniques**



Source: World Bank

more categories. This highlights the need for all stakeholders to work together to prevent fraud, rather than relying solely on regulation, scheme rules, or technology.

4.1 SCHEME RULES

Scheme rules are useful tools to prevent fraud, limiting the effects of fraud when it does occur and aiding in the recovery of stolen funds. At the scheme level, transaction limits (on the value of transactions as well as the number of transactions), allowing holds for further analysis, mandated fraud reporting to the infrastructure operator, and mandated dispute resolution are all helpful in preventing fraud. These approaches may be used in conjunction with one another and are often most effective when implemented in a coordinated manner.

Transaction Limits

There are two types of transaction limits and two sources of these limits. First, there can be limits on the number of transactions that can be made over a given period (hourly, daily, weekly, monthly, and so on). Transaction limits are often used by PSPs but can be mandated by scheme operators as well. Second, there can be limits on the value of each transaction or the total value of a set of transactions initiated over a given period. When the value of an individual or group of transactions is limited, how much bad actors can steal per account takeover is limited.

In Colombia, for example, Transfiya, has put in place scheme rules limiting the number of transactions that can be made each week, whereas almost every other market also has limits on the value of a given transaction. (For example, RTP in the United States limits transactions to $1 million, while the limit for SCT Inst in Europe is €100,000.) One of the negative aspects of both volume and value limits is the way that they may reduce the utility of the system for certain use cases. Business-to-business payments typically require higher value limits to be useful for supplier payments, for example.

Transaction Holds for Further Analysis

Another key anti-fraud tool at the scheme level is allowing service-level agreements to be relaxed when the sending or receiving financial institution (FI) has reason to suspect fraud. This implies an inherent tradeoff between user experience and fraud mitigation. If too many transactions are held, user experience may be harmed significantly. However, if too few suspected fraudulent transactions are held, fraud could become a systemic problem and undermine user trust in the system.

Allowing PSPs to put a transaction on hold can provide sufficient time to investigate a transaction. Most transactions cannot be investigated, so the automation of processes such as anti-money-laundering, counter-terrorist financing, and sanctions-screening checks is necessary. However, the lack of structured data can also result in false positives. This is where the use of transaction holds can help solve many problems. In Mexico, for example, SPEI's rules mandate that participants automate these processes. Similarly, in Brazil Pix notifies senders when their transactions are put on hold.

Fraud Reporting to the FPS Operator

Anti-fraud software typically requires a significant amount of data. While FPS operators have access to transaction-level data, they do not know which transactions are legitimate and which are fraudulent. Requiring PSPs to report fraud to the FPS operator helps solve this problem. Both RTP in the United States, which is owned and operated by the Clearing House, and the New Payments Platform in Australia require PSPs to report fraud. Since November 2023, Brazil's central bank, the Banco Central do Brasil (BCB), has been requiring PSPs to share fraud-related data. Depending on the type of data being shared and local legislation, some type of anonymity or even consent could be required.

In addition, the FPS operator could play a role in instituting a fraud-management program for scheme participants. In the card industry, for example, Visa and Mastercard use mandatory fraud reporting to track acquirers who originate fraud above a certain threshold. Acquirers and processors are typically required to provide monthly reports on their merchants' activities, especially those with high levels of fraud or chargebacks. If the thresholds are exceeded and not corrected, acquirers may face penalties or suspension from the network.

Mandated Dispute Resolution

Mandated dispute-resolution frameworks offer several potential benefits for fraud prevention and resolution. They create clear guidelines regarding consumer liability, ensure common reporting mechanisms, and help to standardize recovery mechanisms. Most frameworks are composed of three components: a structured reporting channel that empowers consumers to start the resolution process as early as possible, an established set of guidelines regarding liability, and damage compensation mechanisms. Each is crucial and helps prevent the formation of perverse incentives/moral hazards for both parties, such as friendly fraud and a lack of compensation from FIs for circumstances of legitimate fraud.

4.2 TECHNOLOGY SOLUTIONS

The core of anti-fraud work in A2A payment systems, including FPS, is carried out using technology. This technology sits at multiple levels along the payment value chain, though chiefly at the level of the PSP (both sending and receiving) and FPS operator.

Centralized Fraud-Prevention Solutions

Over recent years, FPS operators have increasingly implemented centralized fraud solutions. In some cases, these systems score transactions and send alerts to the sending and receiving PSPs. In other cases, operators include information-sharing solutions that, when combined with requirements that PSPs notify operators of fraudulent transactions, can offer additional protection to consumers. While systems that track money mules may not stop fraudulent transactions, they do help in recovering funds and identifying a larger network involved in stealing and laundering money.

Fraud and risk scoring. FPS operators have transparency into all incoming and outgoing payments and therefore have a more complete view of any given transaction than either the sending or receiving party. A scoring or "flagging" system operated by the FPS operator can alert the sending and receiving PSPs given certain conditions, using its central position and access to information that the other parties involved in the payment do not have. In some markets, the operator for A2A payments, such as STET in France, also processes card payments, providing even more data that can be used to detect fraud. FPS operators in other markets, including India, Nigeria, and South Africa, have also centralized fraud-detection capabilities.

Information sharing. On top of offering fraud-scoring solutions, various FPS operators also maintain information-sharing platforms. These platforms offer a range of different services, including the ability to report suspected scammers and potentially fraudulent transactions. While the two types of solutions are theoretically distinct, they work well together and may be offered together. Australia's New Payments Platform has a data-sharing service, as does Iberpay in Spain. Another example is the upcoming FPAD system created by EBA Clearing in the Eurozone.

Money mule accounts detection. Money mule accounts are accounts that move money around—both receiving and sending—on behalf of fraudsters. The Mule Insights Tactical Solution (MITS) in the United Kingdom, developed by VocaLink/Mastercard, offers an example of a service that detects money mule accounts. The system accesses and uses data from the local batch system and FPS to track how money moves between accounts. MITS uses algorithms and machine learning to identify suspected money mules, alert the PSPs that house these accounts, and track funds as they move through the system.

PSP-Based Fraud-Detection Systems

FPS participants across the globe have also implemented their own fraud-detection systems, and PSPs have made substantial progress in this area over the last five to ten years. In some cases, FPS scheme rules mandate that PSPs must have their own fraud-detection capabilities (as in RTP in the United States and Pix in Brazil), but there can be substantial differences in the quality of these systems. The amount of information that PSPs have about their own customers can be substantial, whether the bank has been around for hundreds of years or is a digital-only bank in operation for a few years. While these systems enable PSPs to monitor their own customers on both the sending and the receiving side, information asymmetries—if the PSP is the recipient of a payment, the amount of information it has about the sender is minimal—mean that a centralized system is needed to fill the knowledge gaps.

Risk-based authentication relies on the use of transactional data (for example, location, device, user profile, log-in patterns, and others) to authenticate the user. The data serves as an input for assigning a risk score that can be used to identify risky or low-risk transactions and trigger additional authentication measures, if needed. In markets where MFA is mandated, risk-based authentication is often used as a tool for additional screening or to provide another layer of security. In Mexico, the regulator has mandated that account providers consider the user's geolocation for allowing access to online banking services. In the European Union, transaction risk analysis is used as part of the decision-making process when considering exemptions to strong customer authentication (SCA).[5]

Confirmation of Payee

The rise of APP fraud has forced regulators to come up with ways to provide payment senders with additional information while balancing the need for privacy. Confirmation-of-Payee (CoP) in the United Kingdom was first mandated for large banks but is now becoming more widespread. Over the last several years, various alias-based payment services, such as Bizum in Spain, Swish in Sweden, UPI in India, and PayID in Australia, have begun sharing some level of beneficiary information with senders. Despite the potential benefits of CoP, the system needs to be pro-

tected from abuse. For example, a hacker may try to mine alias directories to get personal information and then use this information to perpetrate other types of fraud. Alias directories and CoP schemes need to balance the ability to retrieve information to protect senders from criminals while also ensuring that confidential information is protected. In some markets, such as CoDi in Mexico, there is a mandatory cooling-off period during which recently added aliases tied to a bank account cannot be paid directly after a potential payer adds the alias to a phonebook.

Digital ID

Digital ID services are also being used more and more to authenticate senders of fast payments. The use of a digital ID featuring biometric information (facial scans, thumbprint scans, iris scans, and so on) is often part of MFA, although this need not always be the case. These systems, such as BankID in Sweden and Norway, It's Me in Belgium, SAVI in Mexico, iDIN in the Netherlands, and Aadhaar in India, ensure that the individual initiating a payment is the individual authorized to make a payment. These services require a significant amount of cross-industry cooperation and are often especially complex to implement.

4.3 REGULATION

Technology and scheme rules can go a long way toward preventing, detecting, and tracking fraud as it moves through the financial system. However, regulation is also imperative to establish the standards that FIs and scheme rules abide by, to provide additional protections to end users of payment systems, and to create opportunities for system stakeholders to try out new technologies and rules.

In some markets, regulators have required FIs to have anti-fraud engines integrated within their payment-processing systems (for example, Pix in Brazil), mandated the use of tools such as CoP or IBAN Name Check (the United Kingdom and European Union, respectively), or implemented cool-down periods when adding new recipients via an alias-based system (CoDi in Mexico). Many countries have also begun requiring that fraud be centrally reported, enabling regulators to collect, collate, and distribute information about fraud to all participants. In other markets, fraud losses have led regulators and/or payment communities to create new mechanisms to distribute the burden of consumer fraud losses. In the United Kingdom, the PSR has mandated that any fraud-based losses be split 50/50 between the sending and receiving PSPs. This aims to provide an incentive to all players to do as much as they can to prevent fraud, both authorized and unauthorized.

Across various markets, the development of common fraud-reporting systems across platforms is a growing trend. For example, the Monetary Authority of Singapore recently announced the development of COSMIC, a secure digital platform (and enabling regulatory framework) that allows FIs to share information about customers who exhibit multiple "red flags" if certain conditions are met. As a centralized platform, COSMIC allows information to be shared in a structured format and specifies how and when certain information should be shared.

The rise of phishing and cyberattacks has made simple "username and password"–based logins too insecure. MFA is widely considered a best practice in terms of authenticating a user prior to payment initiation. This can take many forms. In the European Union, the Revised Payment Services Directive (PSD2) mandates MFA (referred to locally as SCA) for payments above €30 (about $35). To fulfill MFA requirements, two of three types of factors must be used: something someone knows (such as a password or PIN), something someone has (a bound device), or something someone is (a thumbprint, facial scan, and the like). MFA is not foolproof, however, as is shown by SIM swapping (that is, moving a phone number onto a new SIM card controlled by scammers to intercept OTPs sent to authenticate a user). Markets outside the European Union—namely, Mexico, Pakistan, and the United Kingdom—also mandate MFA for different types of transactions.

Last, the use of new technology comes with problems and challenges that need to be ironed out. This can be difficult when considering issues such as data privacy, strict service-level agreements, and application programming interfaces. In India, for example, the government has created a regulatory sandbox that enables PSPs to test out new technology. This environment has been used specifically to encourage the development of new fraud-prevention tools. The use of sandbox environments can help PSPs test solutions, discover shortcomings, create new fixes, and try new technology; taking these steps would be much more difficult without a helpful testing environment. These sandboxes are not used just for fraud-prevention purposes and are quite common in other areas of the financial sector, such as open banking testing platforms.

4.4 CROSS-INDUSTRY INITIATIVES

Scheme rules, technology, and regulation are not alone in deterring fraudsters. Other initiatives, such as fraudulent individuals databases, cross-industry collaboration, and fraud-awareness campaigns/end-user education are also part of the complex anti-fraud puzzle. As mentioned pre-

viously, FPS operators can be involved in information sharing between participants. This can take the form of alerts and enable real-time information sharing, but it can also take the form of a callable database that stores, updates, and maintains information about fraudulent individuals. This database could be operated by the FPS operator or another party, such as a regulator, banking association, payment association, and so on. In Brazil, for example, participants are required to provide feedback on Pix transactions involved in fraud. This also leads to aliases being flagged for fraud purposes, which serves as a de facto watch list or even a form of blacklisting. The Netherlands, Nigeria, and Japan also have forms of fraudulent individuals databases that help with anti-fraud efforts. The actual form the database takes, who has access to the database, how data gets submitted to it, and who can update or amend data are all important questions that need to be answered.

In some markets, education campaigns are created to raise awareness about a specific type of fraud, potentially leading to standardized information about fraud being shared through the industry, as in the Netherlands. In the United Kingdom, the campaign "Take 5—To Stop Fraud" was created to educate the public about fraud and APP fraud. In the European Union, an outstanding proposal for the forthcoming PSD3 includes a provision making fraud-prevention education material mandatory for PSPs. Education also needs to be seen as an ongoing issue, rather than a one-off action that can be crossed off the to-do list.

Fraud is not just a financial industry issue; businesses and individuals are affected by phishing and cyberattacks daily. In some cases, such as SIM swap fraud, vulnerabilities are exploited that can have consequences for end users in the financial sphere. When people call their telephone company, they are often asked a series of questions to verify their identity. These questions, however, are often relatively easy to answer using information gleaned by scanning social media accounts or hacking into someone's email. This means that, short of some type of digital ID or face-to-face interaction, it can be very difficult for the employees of telecommunications firms to be 100 percent sure with whom they are speaking. Using a digital ID to verify the caller's identity could help solve these problems. Another option is to put a marker into a directory when a phone number linked to a bank account has been moved to a new SIM card, which is done in Nigeria for USSD-based payments. A third option, being pursued in the United Kingdom, is for telecommunications companies to block fraudulent SMS IDs.

4.5 INSIGHTS FROM CARDS AND OTHER PAYMENT METHODS

While fast payments are a relatively new payment method, cards, checks, and batch payments have all been around for several decades. It is therefore useful to consider whether they offer any relevant lessons for fraud prevention in fast payments. For example, like fast payments, cards offer real-time authorization and have been doing so for decades. Cards are tied to an account, although not necessarily a transaction account as with fast payments. Banks and network operators have gained considerable experience and expertise in analyzing transaction data from cards, using algorithms to give a transaction a score, determining whether it is fraudulent, and sending the information back. The way that payment data is structured in cards is very different, however: PAN versus account number, ISO 8583 versus (typically) 20022. MFA also originated in the card space and moved over into A2A payments. While there are ways around MFA—such as man-in-the-middle attacks or scams in which fraudsters convince people that the scammers are from the bank and need consumers to provide their OTPs to do something (thereby enabling the fraud to take place)—every step in the security chain makes fraud more difficult to perpetrate.

Even though cards and fast payments are processed on different payment rails, much of the expertise gained in implementing real-time scoring and data checks is transferable to the fast payments space. In some cases, data from the card space can also be used in conjunction with fast payment data to protect end users further. One example of using card-based data in the A2A space is as follows: A consumer uses a card to make a payment in a grocery store. The transaction is authorized using a PIN. Minutes later, a payer from the same account initiates a payment via a mobile device from a location nowhere near where the card was used only a few minutes before. Using location data from the card payment, it would be possible to determine with a high level of probability that the card payment was likely the rightful account holder because the transaction was authorized using the PIN. If the mobile payment did not employ MFA, it is more likely to be fraudulent. STET in France, which acts as the automated clearing house and domestic card scheme, offers a fraud-management service that uses card-based data to enrich A2A data with additional information.

5 CASE STUDIES

BRAZIL

Pix is the consumer-facing side of the BCB's alias-based real-time system called SPI. Although Pix was launched only in November 2020, it is one of the most widely used FPS in the world. Criminals take advantage of Pix's high usage rates and lower levels of digital financial literacy within the country. The most common methods of fast payment fraud include social engineering and (sometimes violent) coercion.

The BCB has implemented a comprehensive set of anti-fraud measures for Pix transactions. These measures include deploying anti-fraud technology at the central infrastructure level, adapting scheme rules to combat evolving fraud threats, and promoting industry-wide information sharing. Pix participants are required to operate anti-fraud engines to detect atypical transactions based on user profiles. Participants are permitted to reject transactions deemed insecure and hold transactions for up to 30 minutes during the day or one hour at night to conduct risk analyses and inform clients about the extended processing time. Transaction data is encrypted, and secure communication with SPI is facilitated through an independent network operated by the BCB.

To bolster security, the Transaction Accounts Identifier Directory (DICT), Pix's alias database operated by the BCB, prevents personal information scans, and includes fraud markers for suspicious transactions. This became mandatory in November 2021, and participants must report infringements to the DICT/BCB, leading to system-wide alerts. Additionally, Pix scheme rules allow participants to set transaction limits based on user risk profiles. The BCB limited nighttime transaction values to R$1,000 ($210.51) due to an increase in nighttime fraud. However, users can adjust the time window slightly (between 10 p.m. and 6 a.m.) and request higher limits. Lastly, the Special Reimbursement Mechanism facilitates fund recovery for victims and standardizes return procedures by the receiving PSP.

INDIA

UPI, operated by the National Payments Corporation of India (NPCI),[6] is India's mobile-based real-time system. Transactions are initiated via mobile devices, with users authenticating themselves using MFA, device binding, and a UPI PIN. As with many other markets, scammers use a variety of methods to perpetrate fraud, including fake payment links asking for money transfers, fake websites and apps, and impersonating bank employees asking for confidential information.

To prevent UPI-based fraud, NPCI offers a real-time solution for monitoring and managing fraud risk as a service to participants. The solution employs artificial intelligence and machine learning to process transactions in real time and generate alerts. As part of the UPI framework, all participants are also required to establish a dispute-redressal mechanism. This allows end users to raise complaints regarding UPI transactions directly through the PSP's app, streamlining the dispute-resolution process.

Additionally, NPCI recommends that system participants implement additional security measures, including velocity checks and transaction limits. Velocity checks involve monitoring the number of transactions initiated from a single account, while transaction limits restrict the number of

transactions initiated from the same account. UPI has also introduced a CoP feature, enabling payers to verify payee details before submitting payments.

In the interest of tackling fraud, the Reserve Bank of India established the Central Fraud Registry. This centralized tool collects and utilizes various data points, allowing FIs to access crucial information, such as perpetrator details, transaction amounts, and dates. This helps FIs ensure that their customers do not send money to suspected fraudsters and provides warnings if a customer has a history of fraud. To streamline fraud reporting, the Central Payments Fraud Information Registry module was migrated to DAKSH, the bank's advanced supervisory monitoring system, in January 2023. This migration signaled a pivotal advance in India's digital ID system, Aadhaar, and also plays an important role in instantly verifying identities at commercial banks, reducing the risk of identity theft. Other initiatives in the country include a regulatory sandbox focused on preventing and mitigating financial fraud, and awareness campaigns using advertisements and customer-orientation programs. In addition, the industry places a special emphasis on conducting awareness campaigns in local languages to educate individuals in rural areas.

MEXICO

SPEI, Mexico's FPS, is one of the oldest in the world, having launched in 2004. The system is owned and operated by Banxico, Mexico's central bank. Given the age of SPEI, Banxico has needed to make incremental changes in response to changing demands, global trends, and cyberattacks. More specifically, SPEI participants' payment gateways were the target of a cyberattack in 2018, though the hackers were not able to break into SPEI itself.

As a result, system participants are now required to establish collaboration agreements that outline procedures for fund recovery in cases of fraud. Reporting suspicious activities and implementing digital signatures for all SPEI transactions are also mandatory. To ensure the system's safety, participants must also utilize encrypted communications when connecting to SPEI. For larger transactions (Mex$50,000/$2,951), system participants can request extended processing time from Banxico for additional fraud and anti-money-laundering checks. To minimize fraud risks, users are also barred from additional withdrawals above this cap on the day the transaction is made.

On the systemic level, CNBV, the Mexican financial regulator, requires MFA during payment initiation to access/authorize all electronic transactions (batch and fast payments). Users of online banking services are also required to share geolocation data as an added security measure. To bolster faster payment growth, Banxico is currently developing an authentication and identity-verification system referred to as SAVI. This system will be used as a central registry of biometric, personal, and transactional data to support user authentication before payment initiation via SPEI.

NIGERIA

Over the past decade, Nigeria has witnessed significant changes in payment habits, with a notable shift toward digitalization. However, this transformation has also raised concerns around mobile payment fraud, particularly through USSD phones[7] and advance fee scams. In response, the Central Bank of Nigeria has taken substantial steps to prevent fraud, including issuing guidelines on transaction value limits for fast payments and mandating that FIs implement a fraud-monitoring system based on behavioral monitoring, pattern detection, and the ability to hold or block suspicious transactions.

The Nigerian Inter-Bank Settlement System (NIBSS), the central bank's RTGS system, also plays a key role in fraud prevention—namely, through an anti-fraud solution that monitors all interbank transactions initiated electronically, including those processed in NIP (NIBSS Instant Payments), the country's FPS. NIBSS operates 24/7, just like NIP, and features the Name Enquiry Service, comparable to CoP in the United Kingdom. The Name Enquiry Service allows a payer to confirm the accuracy of the payee's details before confirming a transaction, so it combats some types of APP fraud. The Name Enquiry Service also includes a picture of the payee.[8]

To address historic, know-your-customer and fraud challenges, Nigeria's banking industry collectively introduced the Bank Verification Number (BVN). The BVN is a biometric identification system aimed at minimizing the risk of fraudulent transactions by assigning a unique ID number to each financial user. Biometric details such as fingerprints and facial scans are associated with the BVN and serve to authenticate users when initiating transactions, like the biometrics used in Scandinavia. Another joint effort between the Central Bank of Nigeria and NIBSS resulted in the creation of the fraudulent individual watch list, containing the BVNs of confirmed cheats. Banks can consult the list before a transaction is made and alert consumers before they make a payment to a known fraudster, further bolstering fraud-prevention efforts.

PAKISTAN

The State Bank of Pakistan (SBP) owns and operates the alias-based FPS known as RAAST, launched in 2022. The FPS was born out of a collaboration between the SBP and Karandaaz, a nonprofit organization that promotes financial inclusion. RAAST is the nation's first electronic payment system that enables end-to-end payments among individuals, businesses, and government entities.

Scheme participation rules for RAAST mandate robust information security policies, standards, and controls for the SBP and system participants to ensure data confidentiality and integrity within the system. Encryption is also mandatory for all payment information. RAAST also possesses a centralized fraud-detection solution, although security measures are applied across the entire system, including network, infrastructure, and applications, to prevent unauthorized access. Participants must actively monitor and report fraudulent transactions, collaborating with the SBP and others for resolution. If fraudulent activities are suspected, alias deregistration or account suspension is obligatory. Sending participants automate fraud and anti-money-laundering checks to meet stringent service-level agreements. Account providers verify users' identities through OTP before initiating payments, and RAAST offers a CoP solution.

The SBP is actively committed to enhancing the cyber resilience of financial market infrastructures through various strategic initiatives. These measures include making MFA mandatory for all digital banking channels, ensuring that customers receive free transaction alerts on their mobile phones for all digital transactions, and enabling complaint-registration options via mobile apps, call centers, and online banking services. These eliminate the need for users to visit physical bank branches. The SBP has also mandated that banks deploy real-time fraud-monitoring tools and encourages banks to put in place customer-awareness campaigns.

SELECT EURO AREA EXAMPLES

The Single Euro Payments Area (SEPA) is uniquely more complex than other markets. Each market must comply with the common rule book for payments as well as its own individual national regulations. Consequentially, some basic standards are set at the SEPA level, while national regulators may expand upon these baseline regulations, provided that doing so doesn't disadvantage other players within SEPA not in the local market. The European Union has continuously strengthened consumer protections against fraud in the rules that set up SEPA (the original Payment Services Directive, or PSD) and PSD2 via regulations requiring SCA. New anti-fraud developments are on the horizon as well, such as the required IBAN Name Check, which will cut down on misdirected payments (both genuinely misdirected as well as fraudulent payments) by informing the sender whether the name on the account being paid matches the name the sender intends to pay.[9] PSD3, which is widely expected to be passed soon, will require the development of a framework for PSPs to share fraud-related data[10] and create customer-education campaigns. This is all in addition to what the individual regulators require of players.

On the national level, several markets have taken innovative approaches to fraud mitigation. Iberpay, the Spanish operator of the domestic FPS, offers a fraud-prevention system that utilizes participant-level information sharing.[11] Individual participants are required to analyze their data and determine when fraud has occurred, but the system allows them to share this information with other participants, aiding in fund recovery and cutting down on money mule laundering. STET, the French equivalent of Iberpay, combines A2A payment information with card data. STET processes card payments for the domestic card scheme and has access to significantly more and different types of data than other FPS operators. The system uses sophisticated algorithms to create risk scores for instant payments.[12] EBA Clearing, the pan-European FPS operator of the batch (STEP2) and FPS (RT1), has announced the creation of the Fraud Pattern and Anomaly Detection (FPAD) solution. FPAD will be rolled out in phases and consists of anti-fraud tools such as CoP and provides network-level insights into fraud.

The Dutch payments community has implemented innovative anti-fraud measures within their national market. The banking community in the Netherlands developed consumer fraud-awareness campaigns,[13] and sender institutions are using an empty field in the ISO 20022 payment message to share concerns around a specific payment with the receiving party. The Dutch banking community has also helped pioneer the usage of IBAN Name Check technology, having first introduced it in 2017, leading to an 81 percent reduction in fast payments fraud between 2017 and 2021. Other markets, including Belgium, Denmark, the Netherlands, Norway, and Sweden, are utilizing digital ID apps installed on smartphones to authenticate senders before payment initiation.

SOUTH AFRICA

South Africa has two FPS, both operated by BankservAfrica (BSA). These systems are referred to as Real-Time Clearing and the Rapid Payments Programme, known as PayShap. PayShap was launched in March 2023 and supports proxy-

based payments and request-to-pay. Within South Africa, the most common fraud typologies include phishing attacks and social engineering, although SIM swap and USSD fraud have recently become more common in the country.

As the system operator, BSA offers the Transactional Fraud Mitigation Service to augment banks' anti-fraud systems. The service identifies potential transactional fraud in bulk and fast payments in near real time by scanning transactions. Based on defined rules, the system assigns a risk score and sends an alert to the FIs involved, allowing them to investigate further. Initially, only the sending FI had the right to investigate the transaction, but BSA gave beneficiary FIs the right to access the service's information because it could contain useful information and intelligence. The sending bank may also alert its customer if it suspects an unauthorized transaction has been made. The Transactional Fraud Mitigation Service is set up and operated as a value-added service and has a participation agreement separate from that of the payment system itself.

BSA also offers the Account Verification Service, which allows customers to verify the beneficiary's details in a manner like CoP. In a break from CoP service standard practices, the Account Verification Service charges a fee for end users. PayShap also has CoP functionality to prevent fraudulent or misdirected payments, as well as transaction value limits and daily limits. Both help limit the potential losses when fraud does occur. Other initiatives include the Southern African Fraud Prevention Service's fraudster database, which is used as a source of information about confirmed scammers within the wider region. These systemic initiatives contribute to a more secure payment ecosystem for consumers and FIs.

THAILAND

The Bank of Thailand, the country's central bank, has been active due to the evolving forms of fraud in the country[14] and has taken measures to strengthen security. Due to the prevalence of phishing attacks, FIs must refrain from sending links requiring user information via SMS and email. FIs are now also required to notify mobile banking users before every transaction and provide a 24/7 hotline to report incidents. The bank is also requiring FIs to have a system that detects suspicious transactions and temporarily freezes transactions upon detection to cut down on the use of money mules.

Digital ID, authentication, and authorization are all utilized in Thailand as well. In the interest of fraud mitigation, FIs in Thailand are advised to require the use of biometrics to authenticate users when opening new bank accounts and making transactions above B 50,000 ($1,459). The Bank of Thailand issued guidelines for FIs to test their solutions in a safe regulatory sandbox set up by the bank. The NDID Platform, set up by the National Digital ID Company Ltd. in cooperation with the Thailand Revenue Department, the central bank, and commercial banks, is a digital ID system used for opening bank accounts.[15]

Industry-wide collaboration is also a key component of the various anti-fraud measures used in Thailand. FIs share information using the Central Fraud Registry, a platform for data sharing regarding mule accounts and suspicious transactions. More than 15 banks have also collaborated to develop an app-based alert service to update users on developments in cybercrime, while the National Broadcasting and Telecommunications Commission and service providers have blocked over 167,000 suspect phone numbers. Telecommunications service providers are allowed to exchange information and allow the police and other authorities to access this information.

UNITED KINGDOM

A2A payment fraud, and especially APP fraud, have been a growing issue in the United Kingdom; these scams resulted in over £1.2 million ($1.55 million) being stolen in 2022 alone. APP fraud accounted for 40 percent of financial fraud losses in 2022, with card-based fraud accounting for 45 percent. APP fraud typically uses Faster Payments, the United Kingdom's FPS. Stakeholders, including the PSR, Pay.UK (the FPS operator and CoP service manager), and UK Finance, an industry association, have worked together on several solutions.

To combat money mule accounts and trace illicit funds within the FPS and batch system, Mastercard/VocaLink, the technical provider of Faster Payments, created MITS using machine learning and advanced analytics. This tool effectively aids FIs in identifying, freezing, and closing money mule accounts as they move throughout the United Kingdom's payment infrastructure.

CoP is another crucial tool in the United Kingdom's ongoing fight against payment fraud. By verifying that the name input into a payment message corresponds with the name associated with the recipient's account, CoP can help fight many types of APP fraud, specifically where the fraudster has convinced the victim that the imposter is someone else, such as a friend, relative, or colleague. While CoP doesn't prevent all types of APP fraud or unauthorized fraud, the PSR has mandated its implementation for about 400 PSPs, extending coverage across the country. Pay.UK is also devel-

oping an information-sharing platform as a part of its larger anti-fraud initiatives.

Furthermore, the PSR took the lead in developing a voluntary industry code, the Contingent Reimbursement Model (also known as the APP Code), which helps victims recover lost funds from APP scams. This new code incentivizes cooperation between sending and receiving FIs by mandating that both parties split the bill for reimbursing fraud victims. This stands in contrast to the voluntary code that was in place before, leaving many consumers unprotected. In addition to the Contingent Reimbursement Model, the PSR is also increasing transparency regarding fraud rates by sharing fraud-related data for PSPs as a part of a "naming and shaming" strategy. Together, these collaborative efforts and anti-fraud measures are bolstering the United Kingdom's resistance to payment fraud, though further steps are still needed.

6 LESSONS LEARNED AND BEST PRACTICES

All the countries discussed in section 5 demonstrate key lessons and/or best practices. For example, Pix in Brazil and UPI in India are two of the most widely used FPS in the world, and fraud was a problem for them at various points in their development. In Brazil, PSPs can attach a fraud marker to aliases within the DICT when fraud occurs, warning other PSPs when sending/receiving payments from/to an account linked to said alias. In India, NPCI has required PSPs to offer dispute-resolution services for fraud victims, which provides a sense of security for end users that there is something that can be done if fraud does occur.

The use of artificial intelligence and machine learning should be seen as a best practice for PSPs and FPS operators alike. FPS operators have access to both sides of a transaction and therefore are well positioned to score transactions and alert PSPs of odd behavior. Likewise, PSPs are privy to unprecedented amounts of data on their customers, both related and unrelated to transaction data itself. Artificial intelligence and machine learning should be used to create end-user profiles that outgoing or incoming transactions can then be checked against for purposes of identifying anomalous behavior.

Various markets have some type of fraudster database, require PSPs to report fraud and share that with the wider community, or have some type of information-sharing system. This should also be identified as a basic requirement, if not necessarily a best practice. The use of aliases and the sharing of data, such as through a CoP solution, can not only help the adoption of fast payments but also help protect end users from some types of APP fraud. MFA is another tool that should be considered a best practice, even if the exact parameters are different due to privacy regulations. Furthermore, fraud mitigation is not a zero-sum game, where PSPs do not cooperate at the market level to prevent fraud from occurring at other PSPs. Scammers will always search for the weakest link; it is imperative that communities work together in appropriate areas to secure the financial system.

Digital ID is one key area where the financial community relies on other stakeholders. Digital ID can go a long way to protecting users from account takeover/unauthorized payment fraud. While by no means foolproof, the use of digital IDs as part of an MFA regime, fraud detection at the PSP and FPS operator level, and end-user education about scams/authorized fraud can significantly prevent fraud.

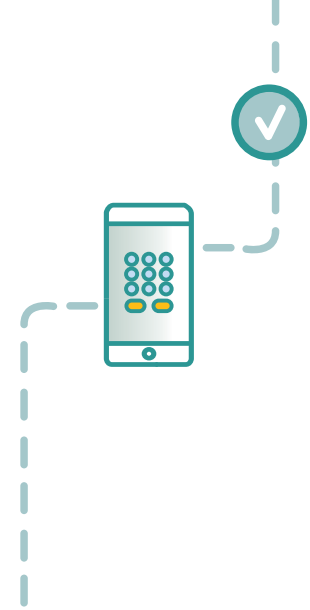
In the dynamic fast payments landscape, a comprehensive campaign to combat fraud requires the concerted efforts of a diverse coalition, encompassing regulators, FPS operators, FIs, and end users. Together, these stakeholders form an intricate tapestry of vigilance, innovation, and cooperation, weaving the fabric of security that safeguards the future of fast payments.

TABLE 2 **The Roles of Ecosystem Actors in Fraud Prevention**

	Regulators	FPS operators	Financial institutions	End-users
Role in fraud mitigation	Setting and enforcing security standards, monitoring compliance, and facilitating cross-industry stakeholder collaboration	System operators are primarily responsible for security infrastructure maintenance and enhancement, transaction monitoring, and facilitating information sharing among participants to enable quick fraud identification and response.	Implementing stringent security measures, conducting customer due diligence, and promptly detecting and reporting suspicious transactions to authorities.	Stay informed, adopt secure practices, and promptly report fraud to PSPs and appropriate authorities.
Examples of fraud mitigation strategies	Development of security standards for PSPs and the operator, development of end-user protections including limiting the liability of customers, mandatory MFA.	Scheme rules such as transaction limits, mandated fraud reporting, and mandated dispute resolution. Implementation of centralized fraud detection, money mule account detection, and information-sharing platforms.	Use of secure authentication methods like MFA, implementation of fraud detection and scoring software, confirmation-of-payee, participating in information-sharing initiatives, and fraud reporting to the regulator.	Participation in fraud awareness and digital literacy programs, limited sharing of personal information, adoption of MFA when possible, and practicing secure password management.

7 CONCLUSION

Fraud has been around since the dawn of payments and is not likely to disappear any time soon. As has been demonstrated in this paper, stakeholders at all points in the payment value chain have a role to play in detecting, preventing, and mitigating the effects of fraud. Regulators need to evaluate privacy laws and ensure that a balance is struck between protecting an individual's right to privacy and needing to share basic information when making a payment. They should consider their ability to establish a digital ID system and the benefits of doing so, enabling consumers to authenticate themselves whenever the need arises. Scheme owners need to ensure that rules are in place to share information about fraud, that basic concepts such as CoP and MFA are established, and that incentives encourage PSPs to work together to prevent fraud—both individually and as a community. PSPs should ensure that modern technology is employed to detect fraud within their own institution, that consumers receive basic education regarding security, their rights, and common fraud schemes, and that the providers participate in community-wide anti-fraud efforts. Payment system end users, consumers, and businesses need to ensure that they stay informed on the types of fraud prevalent in their country, that they take adequate steps to secure their data, and that they make payments only to entities they trust.



8 ACKNOWLEDGMENTS

Organization	Contributor
Lipis Advisors	Lipis Advisors
World Bank	Harish Natarajan
	Holti Banka
	Nilima Ramteke
	Andrea Monteleone
	Thomas Piveteau

ENDNOTES

1. According to the Committee on Payments and Market Infrastructures, a fast payment is defined as a payment in which the "transmission of the payment message and the availability of 'final' funds to the payee occur in real-time or near-real-time on as near to a 24-hour and seven-day (24/7) basis as possible."
2. Office of Sen. Elizabeth Warren, *Facilitating Fraud: How Consumers Defrauded on Zelle Are Left High and Dry by the Banks That Created It* (Washington, DC: U.S. Senate, 2022), https://www.warren.senate.gov/imo/media/doc/ZELLE%20REPORT%20OCTOBER%202022.pdf.
3. National Institute of Standards and Technology, "Cyber Attack," defined in online glossary, https://csrc.nist.gov/glossary/term/cyber_attack. See also IBM, "What Is a Data Breach?" (web page), https://www.ibm.com/topics/data-breach#:~:text=The%20terms%20'data%20breach'%20and,confidentiality%20of%20data%20is%20compromised.
4. For a detailed description of several forms of malware, see European Payments Council, *2022 Payment Threats and Fraud Trends Report* (Brussels: European Payments Council, 2022).
5. For more details on the European Union's SCA and the available exemptions, see World Bank, *Considerations and Lessons for the Development and Implementation of Fast Payment Systems: Part of the World Bank Fast Payments Toolkit* (Washington, DC: World Bank, 2021). See also the previous note on customer authentication for further explanation of SCA and its application of risk-based authentication.
6. Unified Payments Interface (UPI), https://www.npci.org.in/what-we-do/upi/product-overview.
7. USSD is a communications protocol for two-way real-time communication between a mobile phone and a network operator, using 182-character-long alphanumeric messages.
8. NIBSS, https://nibss-plc.com.ng.
9. According to the European Commission's proposal on PSD3. See European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Payment Services and Electronic Money Services in the Internal Market Amending Directive 98/26/EC and Repealing Directives 2015/2366/EU and 2009/110/EC (Brussels: European Commission, 2023), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0366.
10. According to the European Commission's proposal on PSD3. See European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Payment Services and Electronic Money Services in the Internal Market Amending Directive 98/26/EC and Repealing Directives 2015/2366/EU and 2009/110/EC (Brussels: European Commission, 2023), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0366.
11. Iberpay, https://www.iberpay.es/en/.
12. STET, https://www.stet.eu.
13. See Nederlandse Vereniging van Banken (Dutch Banking Association), veiligbankieren.nl.
14. Such as through SMS, call centers, fraudulent loans, and payment apps.
15. NDID: Digital Identity for All, https://www.ndid.co.th.


WORLD BANK GROUP