Payments System Research Briefing

Combating Authorized Push Payment Scams in Fast Payment Systems

by: Ying Lei Toh

November 15, 2024

Fast payments can help consumers improve their cash flow, but the speed and irrevocability of these payments also make them a target for fraudsters seeking to commit authorized push payment (APP) scams. Combating APP scams is critical to ensuring the safety of fast payments and building and maintaining consumer confidence in fast payment systems.

Fast payments are characterized by around-the-clock services and payment recipients' instant (or near-instant) funds availability, enabling consumers to make and receive payments in a timelier fashion than traditional payment methods. But these characteristics, as well as the irrevocability of interbank settlement for (most) fast payments—meaning that once funds from a fast payment transaction are deposited into a recipient's account, the transaction cannot be reversed—are also attractive to fraudsters.

One prominent type of payment fraud in fast payment systems is authorized push payment (APP) scams, where fraudsters manipulate or deceive individuals into authorizing their financial institutions to push funds from their accounts to accounts controlled by the fraudsters. APP scams can generate substantial losses for fast payment system participants, particularly for consumers who fall victim to them. For example, in 2023, customers at the three largest banks that participate in Zelle—a U.S. person-to-person fast payment network—disputed more than $206 million worth of Zelle transactions as scams, with the scam victims bearing more than 80 percent of losses (U.S. Senate 2024). As fraudsters increasingly leverage technology to expand their operations and create more convincing scams, consumers face a growing risk when using fast payments. Efforts to combat APP scams are thus critical to ensuring the safety of fast payments and building and maintaining consumer confidence in fast payment systems. This *Payments System Research Briefing* provides an overview of APP scams in fast payment systems and discusses measures that fast payment system (FPS) operators and participating financial institutions can adopt to mitigate APP scams.

APP scams in fast payment systems

A payment scam—a form of payment fraud in which the fraudster deceives or manipulates an authorized user of a payment account to achieve financial gain—can be distinguished by whether the scam payment was authorized or unauthorized and whether it was a push or pull payment.[1] In an authorized payment scam, the fraudster tricks the victim (an authorized party) into initiating a payment from their account to the fraudster. In an unauthorized payment scam, the fraudster tricks the victim into providing the fraudster access to their account, and the fraudster (an unauthorized party) makes a payment from the victim's account.[2] A push payment scam is one in which the victim instructs their account provider to transfer (or push) funds to the fraudster's account, while a pull payment scam is one in which the victim provides payment information (such as a debit card number and transfer amount) to the fraudster, and the fraudster's account provider draws on (or pulls) funds from the victim's account. These dimensions allow for four types of payment scams: authorized push, unauthorized push, authorized pull, and unauthorized pull. In fast payment systems, payment scams are generally push scams, either APP or unauthorized.[3]

Although both APP scams and unauthorized push payment scams can result in losses for fast payment users, APP scams particularly have been in the spotlight. Stories abound in the media of fast payment users falling for APP scams.[4] From imposter scams to employment scams to online marketplace scams, articles have illustrated how sophisticated scammers can be and how any consumer can become a victim. Such stories also highlight how consumers are especially exposed to the risks of APP scams in fast payment systems. Unlike an unauthorized payment initiated by a fraudster, which may be detected and stopped by a victim's financial institution, an authorized payment initiated by a victim (to a fraudster) will most likely be executed. Once a scam payment is executed, the victim often has little to no recourse, as the payment is often irrevocable. Funds recovery is highly unlikely, if not impossible, due to the (near) instantaneous availability of funds to the fraudster; by the time a victim realizes they have been scammed, the funds are likely gone. Consumer protection laws in most jurisdictions (including the United States) also do not provide liability protection for victims of APP scams, protecting consumers from fraud liability only if a scam payment was an unauthorized payment made by the fraudster.

While addressing the problem of APP scams in fast payment system is critical for consumer protection, mitigating APP scams is also important from an efficiency perspective. APP scams raise the cost of fast payment transactions to society (and thus reduce the net benefit). When consumers dispute their payments as scams, both the sender's and the recipient's financial institutions need to investigate the disputed payments, requiring resources. If consumers refrain from using faster payments due to fear of APP scams, they must use alternative payment methods, which may provide them fewer benefits or incur them higher costs.

Involvement of FPS operators and participating financial institutions in APP scams

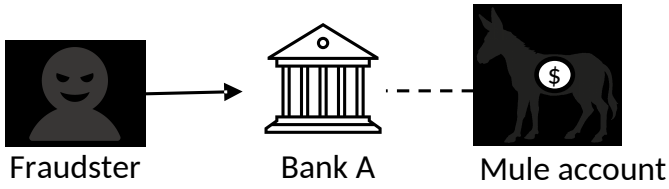
Although consumers ultimately decide whether to initiate a fast payment with an APP scam risk, addressing the issue of APP scams in fast payment systems will likely require more than just greater consumer vigilance. As fraudsters increasingly leverage technology to create scams that appear more realistic, even vigilant consumers may fail to detect them.[5] To effectively mitigate APP scams, FPS operators and participating financial institutions will likely need to play more active roles.

APP scams are typically perpetuated by organized crime groups (like most types of financial fraud), and an organized APP scam operation takes place in three stages: set-up, scam execution, and money laundering.[6] In the set-up stage, fraudsters establish call or data centers and acquire the resources (for example, fake online profiles, caller lists, and bank accounts) needed to execute their scams.[7] Then they establish contact with potential victims and attempt to deceive or manipulate these individuals into sending money to them (execution stage). If the fraudsters succeed in their deception, they proceed to the final stage: money laundering. In this stage, fraudsters or their money mules transfer the scam proceeds out of the accounts that received them or convert the proceeds into other forms of assets.[8] The goal of money laundering is to conceal the origins of their funds, enabling fraudsters to profit from these illicit gains while evading the legal consequences of their crimes (United Nations Office on Drugs and Crimes n.d.).

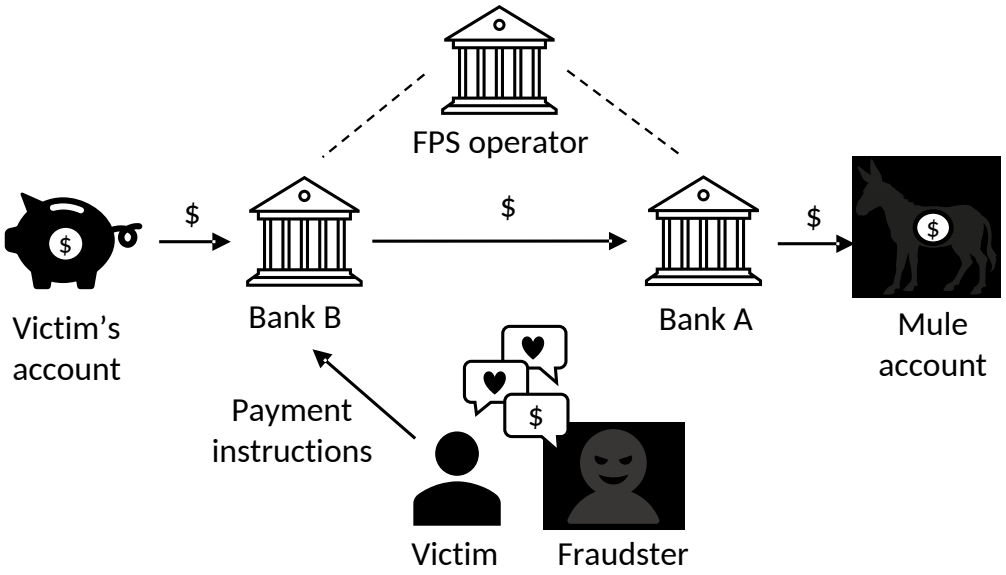
FPS operators and participating financial institutions interact—directly or indirectly—with fraudsters at various stages of an APP scam operation. Figure 1 provides a simple illustration of how the operator and financial institutions (Bank A and Bank B) of a fast payment system may be involved in each stage of an APP scam operation.

Figure 1. Involvement of the FPS operator and participating financial institutions in an APP scam operation

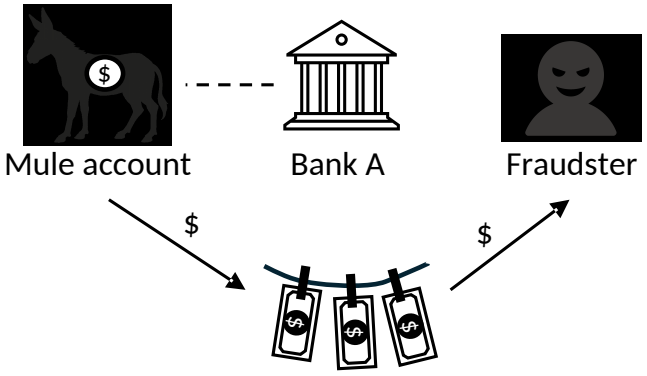
1. Set-up stage



2. Scam execution stage



3. Money laundering stage



In the set-up stage, fraudsters acquire mule accounts—accounts for receiving and laundering scam proceeds—at a participating financial institution (in this case, Bank A). Fraudsters may acquire mule accounts by opening new accounts using stolen or synthetic IDs, purchasing or stealing the account credentials of legitimate bank customers, or recruiting money mules (who may be existing customers of Bank A or may open accounts at Bank A using their real identities under the fraudsters' direction).

In the execution stage, a victim (in Figure 1, of a romance scam) initiates a fast payment from their account at Bank B to the mule account at Bank A. Bank B (the sending financial institution) pushes funds from the victim's account through the fast payment network to Bank A (the receiving financial institution), which then deposits the funds into the mule account. The FPS operator processes the payment and observes the movement of funds across the financial institutions within its network.

In the money laundering stage, the fraudster or their money mule moves funds received from the scam victim out of the mule account at Bank A. This movement of funds is observed by Bank A and may be observed by the FPS operator (if the funds are moved using fast payments or if the FPS operator can observe the movement of funds across payment systems).

Measures FPS operators and participating financial institutions can adopt to combat APP scams

The interactions of an FPS operator and participating financial institutions with fraudsters during the various stages of an APP scam operation present them with opportunities for mitigation. FPS operators and participating financial institutions can adopt different measures at each stage of an APP scam operation to limit scam activities in the fast payment system.

In the set-up stage, participating financial institutions—as potential receiving institutions of fast payments—can adopt measures to prevent fraudsters from obtaining mule accounts, limiting the potential scale of an APP scam operation. Measures include stronger customer identity verification methods, strong customer authentication tools, and educating customers.

Strong customer identity verification methods. Customer identity verification is critical to detecting fraudsters' use of stolen and synthetic IDs to open new accounts. Financial institutions have traditionally relied on documents to verify customer identity, such as a government-issued photo ID. However, fraudsters are increasingly able to leverage technology to evade detection via document verification.[9] To more effectively prevent fraudsters from obtaining mule accounts using stolen or synthetic IDs, participating financial institutions can implement strong customer identity verification methods that rely on factors that cannot be easily falsified by fraudsters. Examples include biometric authentication, behavioral analysis, and digital identity verification.

Strong customer authentication tools. To combat fraudsters taking over accounts of legitimate customers, participating financial institutions can implement strong customer authentication tools such as multi-factor authentication (MFA) and leverage behavioral biometrics. MFA is the use of two or more factors (for instance, a password and a fingerprint) to verify that a customer is who they claim to be.[10] The use of additional factors for customer authentication, particularly factors that fraudsters cannot easily produce (for instance, a customer's biometrics), can make accounts less vulnerable to account takeovers. Behavioral biometrics is the analysis of patterns in user behaviors and activities (for example, scrolling behavior and mouse movement patterns), which can be used to detect anomalies in customer behaviors that may indicate unauthorized access (Rebner 2021).

Customer education (money mules). Individuals who serve as money mules may have been recruited by fraudsters through money mule scams (often disguised as job opportunities) and may not be aware that they are in fact laundering money for fraudsters. Participating financial institutions may be able to prevent some of their customers from becoming money mules by educating them about common money mule scams and the consequences of serving as money mules.

In the scam execution stage, sending financial institutions and FPS operators can implement measures that can help consumers make more informed transaction decisions, thereby lowering the likelihood that they execute scam transactions. Measures include customer education, confirmation of payee functionality, scam risk assessment, and information sharing.

Customer education (APP scams). FPS operators and participating financial institutions—as potential sending institutions—can help reduce the likelihood that consumers fall for APP scams by educating them about common APP scams and red flags.[11] Additionally, participating financial institutions may remind their customers of scam risks and the common signs of scams (for example, through pop-up alerts) when they are initiating a fast payment.

Confirmation of payee (CoP). Sending financial institutions can deploy CoP to help their customer detect scams, especially impersonation scams. CoP is a payee name verification service that enables the sender to verify that the accountholder name on the account they are paying matches that of the intended recipient prior to executing the transaction.[12] FPS operators can play a key role in developing and implementing the CoP functionality in their systems. For instance, the FPS operator in the United Kingdom, Pay.UK, introduced CoP in 2020 as an overlay service to participating financial institutions (Pay.UK 2024).

Transaction scam risk assessment. Sending financial institutions may leverage available information and technology, such as artificial intelligence (AI) and machine learning, to assess the scam risk of a transaction prior to execution and alert their customers if they are about to make a high-risk transaction. For instance, sending financial institutions may use information about the payee's account, when available, to assess whether the account is likely being used for scams.[13] Sending financial institutions may also assess the scam risk of a transaction using behavioral biometrics (which leverage data on a customer's

behavior and machine learning) to detect anomalies that could indicate that the customer is being scammed into making the transaction (Crosman 2024).

FPS operators can develop and provide scam risk assessment tools to participating financial institutions in their systems. The FPS operator has data on all transactions in its system, which can be fed into statistical models to predict scam risks. The use of AI and machine learning models for scam prediction appears to be particularly promising. Earlier this year, Pay.UK concluded a successful pilot of an APP scam detection solution that uses AI to predict scam risks: it detected 56 percent of APP scam transactions, outperforming traditional scam detection models (Featurespace 2024).

Information sharing. Sharing information about suspicious accounts and accounts involved in suspected and reported scam transactions between participating financial institutions can help them prevent customers from falling for APP scams perpetuated using these accounts. Sending financial institutions can alert their customers if they are about to send money to these accounts, which may lead these customers to cancel the potential scam payments. Depending on the rules of the fast payment system, participating financial institutions may also be able to hold payments to these accounts for further risk analysis or create a negative payee list to block all payments to these accounts.[14] Additionally, shared data can be used to train AI and machine learning models to predict scam risks in transactions.

FPS operators can play a central role in facilitating information sharing across participating financial institutions in their system by collecting and disseminating information or establishing a platform for information sharing. In several jurisdictions, FPS operators require participating financial institutions to report scams and suspicious transaction activities to them (Faster Payment Council 2024; World Bank Group 2023).[15]

Finally, in the money laundering stage, receiving financial institutions and FPS operators can adopt measures to detect money laundering activities and take down mule accounts. Measures to detect money laundering activities and identifying mule accounts are critical to preventing fraudsters from continuing to perpetuate scams using these accounts. Timely detection may also prevent fraudsters from successfully laundering their illicit gains and may enable victims' financial institutions to claw back funds that were transferred to the mule accounts.

Transaction monitoring. Receiving financial institutions can monitor their customers' accounts (by leveraging AI and machine learning) for unusual transaction activities or patterns that suggest customers or fraudsters are using accounts for money laundering. The financial institutions can freeze suspect accounts to further investigate and subsequently close accounts if they find evidence of money laundering.

FPS operators can also perform real-time transaction analysis at the system level to detect suspicious transactions and accounts and alert the financial institutions involved so that they can investigate further. The FPS operator is arguably better able to

detect scams than receiving financial institutions, as they have a more comprehensive view of transaction flows across institutions within its system (World Bank Group 2023). Some FPS operators may also be able to combine fast payment transaction data with other payment rails' transaction data, enabling them to track the movement of funds across payment rails. For example, the Mule Insights Technical Solution (MITS) in the United Kingdom traces funds as they move across UK payment systems and uses machine learning to detect suspicious account activities (World Bank Group 2023).

Although all measures discussed here can help combat APP scams and reduce the cost of these scams in fast payment systems, implementing these measures would add to the operating costs of fast payment systems. FPS operators, together with their system participants, could perform cost-benefit assessments to determine whether and how much FPS operators and participating financial institutions should spend on each of these measures. In addition, rules, standards, or a well-designed scam liability policy will likely be necessary to incentivize participating financial institutions to implement the appropriate measures.

Conclusion

APP scams reduce the safety and efficiency of fast payment systems. To mitigate APP scams, FPS operators and participating financial institutions may adopt various measures. Some measures help prevent fraudsters from setting up mule accounts used to conduct scams, some measures help reduce the likelihood that consumers will execute scam payments, and other measures weaken fraudsters' ability to perpetuate more scams.

Although FPS operators and participating financial institutions have important roles in combating APP scams in fast payment systems, their influences are limited to the financial aspects of APP scam operations. To conduct APP scams, fraudsters also often rely on forced labor and abuse telecommunication systems (for instance, by spoofing caller IDs), social networking and dating sites (for instance, by creating fake profiles), online marketplaces (for instance, by creating fake product listings), and so on. To combat APP scams more holistically, cross-industry collaborations between FPS operators and participating financial institutions, telecommunication companies, operators of other digital platforms, and law enforcement agencies will likely be necessary.

Endnotes

[1] Payment fraud is defined as "an action taken with dishonest intent to take something valuable from a payment system participant." This definition can be found in the Glossary of Terms published by the Federal Reserve's Faster and Secure Payments Task Forces.

[2] See the Federal Reserve's ScamClassifier Model for more information on classifying authorized versus unauthorized payment scams.

[3] Most fast payment systems, including those in the United States, only offer push payments.

[4] Figure 4 of the U.S. Senate Permanent Subcommittee of Investigations Majority Staff Report on Zelle provides examples of common Zelle scams (U.S. Senate 2024).

[5] Many fraudsters leverage technologies such as caller ID spoofing, where they manipulate the information transmitted to potential victims' caller IDs to display fake numbers or identities (for example, the name of a government agency), as well as AI voice cloning, where they use AI to create voice clones of the friends or family members of potential victims, increasing the likelihood of the victim falling for the scam.

[6] These stages are adapted from Moody's (2024).

[7] Fraudsters often set up call or data centers in jurisdictions with weaker oversight and employ many individuals, some of whom may be unwitting of the true nature of their employment or forced to work, to assist in their scam operations (Interpol 2024; Moody's 2024).

[8] After the scam proceeds leave the accounts, they may go through a series of other transactions (a process known as layering) before they are reintegrated into the financial system (Dow Jones n.d.).

[9] For instance, some fraudsters now use generative AI to create deepfake documents that they can provide for identity verification purposes, particularly when opening accounts online (Interpol 2024).

[10] Financial institutions can rely on three factors to authenticate a customer: something a customer knows (for example, a password), something a customer has (for example, a one-time PIN delivered to a device the customer owns), and something a customer is (for example, a fingerprint).

[11] An example of such efforts is the education campaign that Zelle launched in partnership with the Better Business Bureau to inform consumers about the signs of payment scams.

[12] CoP may be performed in a few ways. In Hong Kong's Faster Payment System, the sender enters the alias or account number of the intended recipient, and the CoP service returns a partially masked name of the accountholder corresponding to the alias or account number entered. In the UK's Faster Payment System, the sender enters the recipient's name and account number, and the CoP service informs the sender whether the name of the accountholder for the account number entered is a perfect match, close match, no match, or is unavailable for matching with the recipient name the sender provided.

[13] Participating financial institutions in the Zelle network in the United States have access to payee risk attributes through Zelle Risk Insights (Faster Payments Council 2024).

[14] The fast payment system rules in some jurisdictions also allow for sending financial institutions to delay high-value or suspicious transactions for additional risk analysis and set lower transaction limits for high-risk transactions or customers. For example, Brazil's Pix allows participants to hold transactions for up to 30 minutes during the day or one hour at night to perform risk analysis, reject transactions that are not deemed to be secure, and set transaction limits based on their customers' risk profiles. Although transaction limits do not help prevent scams, they can reduce losses if transactions turn out to be scams.

[15] In some jurisdictions (for example India and Thailand), the central bank oversees their jurisdiction's FPS operator and assumes the role of developing and maintaining the information-sharing platform (World Bank Group 2023).

Author

Ying Lei Toh

Senior Economist

Ying Lei Toh is a senior economist in the Economic Research Department at the Federal Reserve Bank of Kansas City. Ms. Toh joined the Bank in 2018, after earning her Ph.D. in Economics at Toulouse School of Economics (TSE), France. She also holds a M.Sc. in Economics from TSE and a B.A. (with Honors) in Economics from Nanyang Technological University, Singapore. Her research focuses on the digital economy---particularly, the issues of consumer privacy, data protection and cyber?security---and the payments market.