Examining Faster Payments Fraud Prevention

U.S. Faster Payments Council

July 2020

Contents

Introduction

The U.S. Faster Payments Council (FPC) formed the Fraud Information Sharing Work Group to identify enhancements that will make the current fraud information sharing processes more efficient and effective. The aim is to foster better user experiences, bolster confidence and trust in Faster Payments, and facilitate faster reaction times to address threats to the ecosystem. The Work Group is composed of team members possessing expertise and experience within Faster Payments in product management, operations, technology, fraud prevention, risk management, and control management.

The Work Group's goals include identifying common definitions for fraud reporting and education, awareness of specific scams and tactics, sharing of fraud prevention techniques, and identifying fraud sharing forums as opportunities for collaboration.

The FPC recognizes that many payment channels are in use including ACH, wire, and cards. While many of the themes and practices in this white paper apply to those, our primary focus is Faster Payments.

Our first deliverable is this white paper addressing the following two areas of Fraud Prevention as they pertain to Faster Payments:

1. Fraud Themes and Trends: Examination of current events to provide clarity and insight
2. Approaches for Mitigating Fraud

This document represents the collective research of the Work Group. There are many external references highlights and we encourage the reader to take advantage of the links to conduct further research.

Fraud Trends Related to Faster Payments

Faster Payments create an attractive target for fraudsters. It has often been stated that "Faster Payments equals faster fraud." While this is often cited, the FPC Fraud Information Sharing Work Group ("Work Group") sought to understand some of the trends that drive fraudsters to this new paradigm and if Faster Payments are a more lucrative target. The Work Group canvassed recent literature and discussed real-life experiences and use cases related to Faster Payments fraud. This research provided a robust collection of information.

To make it more digestible, one of the two subgroups within the Work Group categorized this information into general themes which are further developed in this paper. These themes include:

- Current U.S. Identity Infrastructure is Broken
- Instant/Faster Push Payment Scams
- Social Engineering is a Primary Attack Vector

What follows is a synopsis of the findings of the Work Group.

TREND: Current U.S. Identity Infrastructure is Broken

Digital identity is an electronic compilation of identity attributes digitally captured and stored which provide remote assurance of the identity of a person and can be used in electronic transactions.[1] Improved security measures from payment networks have made payment fraud increasingly difficult to commit on a massive scale; for example, EMV chip cards which prevent cloning of physical cards, tokenization, and EMVCo 3DSecure 2.0[2] continue to improve the security of online payments. As a result, criminals are turning toward stolen or synthetic identity to commit fraud.

It is widely recognized that the digital identity infrastructure in the United States is vulnerable to attack by fraudsters and organized crime due to several factors, including:

1. Exposure of massive amount of Personally Identifiable Information (PII)[3] from frequent data breaches
2. Poor security hygiene among consumers:
    - Sharing PII, attributes, and behavior freely and at times unknowingly, spurred by benefits perceived to exceed the risk
    - Exposing PII and other information on social media that could be used to respond to Knowledge Based Authentication (KBA) questions, e.g., "mother's maiden name"
    - Poor security practices, e.g., password reuse, not applying passcodes or failing to utilize biometric login protections to mobile devices
3. Existing rules and regulations not digitally ready:
    - Lack of ability for financial institutions and others to validate government IDs such as social security numbers (SSNs) matched to name and date of birth (although the Social Security

[1] Digital ID: Driving Global Business Opportunities, Medici, 2020
[2] EMV 3D Secure, EMVCo
[3] Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST

Administration is piloting a new electronic consent-based SSN verification service [eCBSV] in June 2020)[4]
    - Fragmented privacy protection laws regarding sharing of PII
4. Heritage identity verification processes do not accommodate a digital environment:
    - Manual, antiquated, slow, high-friction identity processes in contrast to automated instant payments and fraud perpetration
    - Tools slow to adapt to new threats
    - Siloed nature of fraud vs. Anti-Money Laundering (AML) and Know Your Customer (KYC) teams and processes yielding suboptimal results[5]

How Fraudsters Take Advantage

Fraudsters continually exploit every possible avenue to obtain and use PII and to apply sophisticated machine learning to evolve attack strategies to stay steps ahead of fraud prevention tools. Two of the most common methods fraudsters use are Account Takeover (ATO) and the use of Synthetic Identities.

- **Account Takeover**
    - Use of **phishing** or **man-in-the-middle attacks** to steal account credentials and intercept one-time passcodes to reset account passwords
    - **Credential stuffing:** Automated testing of stolen usernames and passwords at multiple websites with the intent of taking over a large set of accounts all at once[6, 7]
    - Use of stolen or openly available data to **answer Knowledge-Based Authentication (KBA) security questions**
- **Synthetic Identity**
    - Use of a combination of real and fake PII to create a new and believable identity

Rise of Synthetic Identity

Synthetic identity fraud is reported to be the fastest growing type of financial crime in the United States.[8] Synthetic identity fraud occurs when perpetrators combine fictitious and sometimes real information, such as a name and SSN, to create a new identity in one of several ways. Methods used to create synthetic identities include:

- **Identity fabrication:** A completely fictitious identity without any real PII
- **Identity manipulation:** Using slightly modified real PII to create a new identity
- **Identity compilation:** A combination of real and fake PII to form a new identity

Until now, credit bureaus or financial institutions lacked means of matching social security numbers with other PII, creating the opportunity for bad actors to establish credit history for the new identity. These identities may then be used to defraud financial institutions, private industry, government agencies, or individuals. Synthetic identity fraud is often difficult to detect because synthetic identities mimic

[4] Partnering with the SSA to Help Eliminate Synthetic and Modified Identity Fraud, , Early Warning, 2019
[5] How to Marry AML and Fraud, Bank Info Security, 2011
[6] How Hackers Steal Your Reused Passwords: Credential Stuffing, Dashlane, 2017
[7] Your Pa$$word Doesn't Matter, Microsoft, 2019
[8] Synthetic Identity Fraud Is The Fastest Growing Financial Crime -- What Can Banks Do To Fight It?, Forbes, 2019

behavior of legitimate accounts and the resulting fraud is often misclassified as conventional identity theft or a credit loss.

Unlike identity theft, which refers to impersonating a real person, synthetic identities are false, and are often called victimless crimes. However, financial institutions and children are typically impacted. The real SSN used to build up credit often belongs to a child who discovers their ruined credit when they apply for a loan. The funds bad actors steal result in a loss to the financial institution, which impacts its clients and shareholders.

Due to the length of time it takes to build up a good credit history, synthetic identity fraud may go undetected for years. Bad actors obtain credit cards, make purchases, and pay them off, just like a first-time borrower would do. Then, they request increasingly higher limit cards and eventually qualify for traditional loans and mortgages. High-dollar credit cards and loans have been their target. Bad actors take the funds ("bust out") and disappear; there is no real person for the financial institution to collect from. Synthetic Identity Fraud in the U.S. Payments System study describes a crime ring that created enough synthetic identities over a 10-year period to obtain the information of over 25,000 credit cards. The ring busted out by running transactions on merchant terminals obtained by setting up fraudulent businesses.[9]

While difficult to detect, synthetic identities have characteristics that can help identify them. Many of them rely on cross-correlation of SSN or addresses across multiple supposedly unique individuals. Mitigation efforts are evolving, including an effort by the Social Security Administration to improve verification of name and date of birth.[10]

The Federal Reserve Bank of Boston has written extensively on this phenomenon and published three white papers: "Synthetic Identity Fraud in the U.S. Payments System," "Detecting Synthetic Identity Fraud in the U.S. Payments System" and "Mitigating Synthetic Identity Fraud in the U.S., Payments System".[11]

TREND: Faster Push Payment Scams

A fast-growing fraud method that is being perpetrated in this faster payment environment is in the form of an Authorized Push Payment (APP) scam. APP fraud occurs when fraudsters deceive consumers or individuals at a business to send them a payment under false pretenses to a bank account controlled by the fraudster, after which the fraudster transfers the money through a series of accounts in seconds to hide their tracks before the sender has time to realize the deception.[12] Below are a few examples of attacks on consumers and businesses:

- Attacks on consumers:
    - Phony requests for money through a forged invoice or fake email
    - Account takeover through social engineering
- Attacks on businesses:

[9] Synthetic Identity Fraud in the U.S. Payment System A Review of Causes and Contributing Factors, The Federal Reserve, 2019
[10] Consent Based Social Security Number Verification (CBSV) Service, Social Security Administration, 2020
[11] Mitigating Synthetic Identity Fraud in the U.S., Payments System, The Federal Reserve, 2019
[12] What Is Authorized Push Payment Fraud, FICO, 2017

- Hacking into emails to divert mortgage closing payments
- Submitting fake invoices

However the attack occurs, it seeks to take advantage of the nature of Faster Payments: the money may transfer from a customer account within 30 minutes.[13] The speed of which the fraud has been carried out is a primary reason why fraudsters are attacking clients on Faster Payments rails. One article suggests a 24-hour delay for a first-time payment could serve as a means of fraud mitigation.[14] In many cases, fraudsters are not attacking technology; rather, attempting to "dupe" or "deceive" a person into doing their bidding; this approach is called "social engineering."[15]

TREND: Social Engineering is a Primary Attack Vector

Social engineering is an attempt to trick someone into revealing information (e.g., a password) which can then be used to attack systems or networks.[16] Rather than directly attacking any particular authentication technology, bad actors rely on the consumers involved to provide the means to defeat security measures. Social engineering is a key trend not because it is new, but because as security technology and payments methods evolve, fraudsters are always looking for new pretexts on which to tailor their attacks, and new ways to leverage points of human interaction in a system. As authentication technologies get better, the consumer becomes the weakest link when it comes to fraud prevention. Social engineering is less a type of fraud and more a technique used to achieve a goal that leverages cognitive biases to gain access to a system regardless of the technical controls in place.

The major components of a social engineering scam are:

- Method of contact
- Pretext or reason the fraudster uses to initiate the scam
- Method used to bypass security
- Method of extracting funds from the victim

These methods typically follow a cycle of contact, followed by grooming, and then extraction of funds, with requests for action characterized by a sense of urgency.

Social engineering is successful precisely because it relies on human nature. All of us can be susceptible to appeals to ego or authority. We generally desire to be helpful. We have a built-in fear of incurring loss and are enthusiastic to get free rewards. Scammers rely on these traits, among others, to tailor attacks, and within the context of a faster payment, there is less time to avert them.

Authorized vs. Unauthorized

In some instances, fraudsters use social engineering to access the victim's account, making unauthorized payments, and the rightful owner of the account had no part in making the payment. This can be contrasted with APP Fraud where victims are manipulated into making payments to a destination in

[13] What to do if you're the victim of a bank transfer (APP) scam, Consumer Rights, 2019
[14] Britain's digital payments have gotten too fast, Quartz, 2019
[15] Protect Your Personal Data: Learn to Better Protect Yourself, Barclays, 2019
[16] NIST Computer Security Resource Center – Glossary, NIST, 2020

control of the fraudster. Victims of APP Fraud may create or authorize a transaction to send funds to the fraudster or an accomplice using either a personal or business account under false pretenses.

In the case of authorized but fraudulent transactions, the consumer or business typically bears the burden of the loss. While some financial institutions assess scams involving faster payment transactions on a case-by-case basis before determining if the bank will compensate the customer, others have policies that make the consumer completely liable. This pattern differs from card liability, and institutions report the use of significant employee time when emotional and confused customers realize they have lost significant sums of money. These cases have also been publicized in trade journals and the local and national press, and therefore associated with reputational risk to the financial institution.

Business Email Compromise (BEC)

2019 was the first year that BEC topped the list of sources of fraud attempts and it is concerning how widespread this type of attack has become. BEC compromises led to losses of over $1.7 billion in 2019.[17] According to Special Agent Martin Licciardo, a veteran organized crime investigator at the FBI's Washington Field Office, "BEC is a serious threat on a global scale, and the criminal organizations that perpetrate these frauds are continually honing their techniques to exploit unsuspecting victims."[18] According to the 2019 Association for Financial Professions Payments Fraud and Control Survey Highlights, 80% of organizations experienced business email compromise, while 54% of organizations experienced financial losses as a result of business email compromise in 2018.[19] Between January 1, 2018, and June 30, 2019, the dollar loss associated with Direct Deposit change requests (related to payroll diversion) increased 815%.[20] Another FBI report highlights the heightened threat during the COVID-19 pandemic.[21]

BEC, also known as Email Account Compromise (EAC), exploits the fact that so many rely on email, both personal and professional, to conduct business. Typically, these sophisticated fraud schemes target businesses that perform wire transfers as payments. However, because Faster Payments are also generally irrevocable, the opportunity exists for schemes to evolve which target this payment channel.

The scam is executed by compromising legitimate business email accounts through various hacking type activities. Once compromised, a fraudulent email is sent directing victims to unknowingly conduct authorized transfers of funds. Common patterns of BEC include:

- Fraudsters pretending to be senior executives directing employees to transfer funds into fraudsters' accounts
- Vendors receiving fraudulent emails from their clients' employees requesting a change in payee bank accounts or payment instructions

As faster payment transactions become more available to businesses, the percentage of BEC losses tied to new instant payment methods can be expected to grow.

[17] 2019 Internet Crime Report, FBI, 2019
[18] Business E-Mail Compromise: Cyber-Enabled Financial Fraud on the Rise Globally, FBI, 2017
[19] Payments Fraud and Control Survey Highlights, Association for Financial Professionals, 2019
[20] Business Email Compromise The $26 Billion Scam, FBI, 2019
[21] FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic, FBI, 2020

Other Methods of Attack

Account Takeover (ATO) is the result of a cyber-criminal gaining access to credentials and authentication methodology used to sign into a customer's online banking platform and electronically steal funds.[22] The U.S. Secret Service, the FBI, the IC3, and the Financial Services Information Sharing and Analysis Center (FS-ISAC) jointly released a publication outlining how account takeover is often perpetrated, as well as how to protect, detect, and respond to the this type of fraud. ATO begins by a cyber-criminal using various methodologies to manipulate victims into divulging information necessary to ultimately gain access to an online banking account. These methodologies may include opening a malicious email attachment, accepting friend/follower requests on social media or networking accounts, or visiting websites – even legitimate websites – which may then install malware onto the user's computer. The cyber-criminal's end goal is to infect the user's computer with malware used to monitor the user's activities, including visiting a financial institution's website and entering login credentials. Once the cyber-criminal has this information, they can begin conducting unauthorized transactions using the user's own login credentials.[23]

Phishing attacks use email for initial contact. The email often prompts the user to open an attachment or click a link that will download malware or take the user to a fake site to enter real credentials. Trends in phishing include personalized messages, that might include properly formatted hyperlinks, and websites might have the appropriate branding and user interface.

SMishing is an SMS ("text message") version of a phishing cyber-attack. The fraudsters use SMS instead of email templates to lure recipients into providing credentials via text message reply. As people become more suspicious of phishing attacks, hackers turned to this new technique.[24] Scammers depend on users' trust of SMS messaging to trick them into giving up sensitive data including banking details and credit card details via text or SMS message reply.

Vishing is the voice version of phishing using voice messages to steal identities and financial resources. Threat research conducted by Mimecast[25] found that malicious voicemail messages are not just on the rise, but are "evolving and more nuanced than ever before."

Pretexting in social engineering is the use of a fictional backstory to manipulate someone into providing private information or to influence behavior. Generally, the fraudster is using the story, or pretext to get access to financial or authentication information. An example is when a scammer reports a device as lost, and asks the mobile provider to activate a new SIM card with the victim's phone number.[26] If a customer service agent believes the criminal, the victim's phone number gets activated on the criminal's device. Now they can circumvent two factor authentication via SMS or voice calls to that phone. In addition, many scammers use current events as a hook, or pretext, to perpetuate frauds.

Fraudsters often take advantage of panic, chaos, and speed at which the current environment is changing. Crises and emergencies give rise to a new wave of fraudsters who seek to prey upon an anxious public. The more catastrophic the event, the more active the fraudsters. COVID-19 related frauds have already totaled $13.4 million through the end of March 2020, or 3% of the total $432.4

[22] Account Takeover: What You Need to Know, Nacha, 2017
[23] Fraud Advisory for Businesses: Corporate Account Take Over, Nacha, 2019
[24] How To Protect Yourself From Smishing Attacks in 2020, TechViral, 2020
[25] Vishing Attachs to Become Commonplace in 2020, Infosecurity Magazine, 2019
[26] 2020 fraud trends: Are you prepared for what the future holds?, The Paypers, 2020

million of frauds reported to the FTC for the same period.[27] Emerging fraud involve the creation of fake charities requesting donations and sites promising to provide relief. Fraudsters can also use these sites to harvest sensitive payment information.

Whether COVID-19, stimulus payments, or work-from-home scams, criminals are quick to leverage disasters and uncertainty to get access to consumer and business accounts. A good resource for keeping up with the latest frauds is the FTC Scam Alerts web page. Alerts detail recent scams and outline how to recognize the warning signs.

The features that make instant P2P applications so useful for customers, including speed and ubiquity, have made them targets for thieves.[28] Where there are new products, new flows, and new methods of customer contact, there will be criminals ready to exploit customer trust and confusion. Faster Payments are the newest channel which fraudsters will continue to evolve their strategies to manipulate and defraud consumers and businesses.

[27] Americans have lost $13.4 million to fraud linked to Covid-19, CNBC, 2020
[28] Zelle P2P Fraud: You Ain't Seen Nothing Yet..., Finextra, 2020

Mitigating Fraud

Fraud in payments is not new. As long as payments have existed, bad actors have sought personal gain through attacking weaknesses in how money is moved. Many capabilities have been developed to mitigate fraud in electronic payments. Faster Payments introduce new challenges in protecting the payments from bad actors.

Wire transfers, which have been available for years to move money electronically, are a close analogy to modern Real Time Gross Settlement (RTGS) payments – or indeed any kind of "faster" payment. When a customer is sending a wire, the instruction is irrevocable. This means that when a wire payment is sent, money is taken out of the account and there is no recourse to recover funds. When a wire payment is received, funds are immediately available to the recipient and they have assurance the funds transfer is final.

Given the finality of a wire transfer, financial institutions have implemented fraud mitigation processes around wire transfers. From special enrollment to send a wire, separate wire agreements, authentication and authorization activities when a wire is initiated, and holds placed on funds going out and coming in, financial institutions have inserted many steps to slow down the immediacy of a wire payment in an effort to mitigate fraud.

Users of Faster Payments will not tolerate added friction or reduced speed of a payment as is done with wire transfers. As such, the industry must re-think fraud mitigation. Existing capabilities must be re-evaluated and modernized to support Faster Payments, and new capabilities must be developed. This section highlights a portion of approaches and efforts to modernizing fraud mitigation.

Fraud Classifications

Part of mitigating fraud is understanding the types of fraud that you're trying to mitigate. The Federal Reserve Fed Payments Improvement Fraud Definitions Work Group[29] developed a Fraud Classification Model for Payments. The model outlines 12 categories into which payment fraud is classified. Payment fraud may be performed by an authorized or unauthorized party. Authorized parties commit payment fraud through manipulation, via modified payment information, or intentionally acting fraudulently. Unauthorized parties take over accounts or conduct fraudulent payments by misusing account information. The Fraud Classification Model for Payments figure below outlines each classification and whether it was conducted by an authorized or unauthorized party. All classifications, except Physical Alteration and Physical Forgery/Counterfeit, apply to Faster Payments.

[29] Fraud Definitions Work Group, FedPayments Improvement, 2019

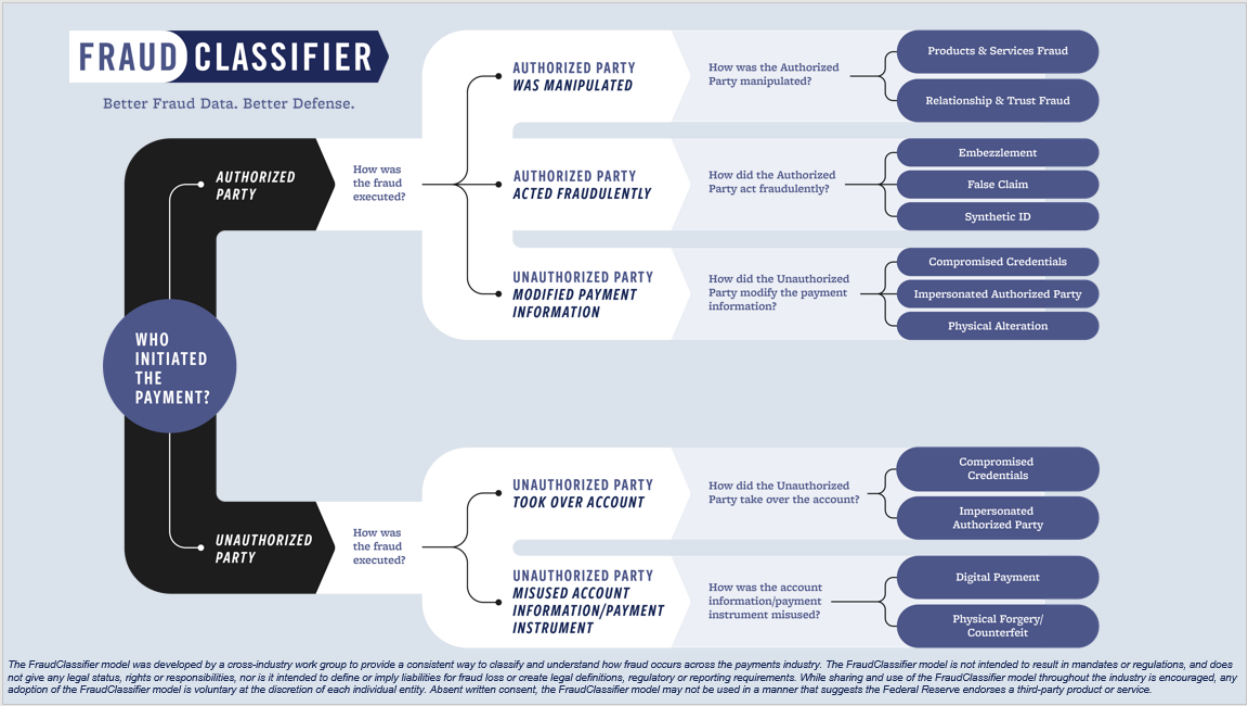

Figure 1: FedPayments Improvement Fraud Classifier Model[30]

Fraud Classification	Mitigation Approaches
Products and Services Fraud	Education is one of the best weapons against fraud. Educate users of current threats and trends. Research the provider of the product or service prior to initiating payment.
Relationship and Trust Fraud	Be alert to opportunities or relationships that are "too good to be true." Users should protect personal information and keep their social media presence safe. Never initiate a payment to a social media counterparty or "friend" you have not met in person. Monitor and enroll financial accounts in alert messaging to identify unauthorized activity.
Embezzlement	Maintain a strong internal control program. Limit the number of individuals with access to initiate Faster Payments. Segregate duties of employees involved in the

[29] https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/, FedPayments Improvement, 2019

	payment process. Reconcile accounts to identify suspicious payments.
Synthetic ID	Implement a robust onboarding process utilizing Artificial Intelligence (AI) and Machine Learning (ML), looking beyond traditional PII. When available, utilize a service such as the SSA's eCBSV.
Impersonated Authorized Party and Compromised Credentials	Require complex passwords and provide Multi-Factor Authentication (MFA), Out-of-Bounds Authentication (OOBA) or Two-Factor Authentication (2FA). Maintain a sound cybersecurity framework. Use identity monitoring services which include dark web monitoring. Verify changes to payment instructions or informational changes with an authorized individual via a trusted source. Never provide your credentials to another party.
Digital Payment	Implement anomaly detection strategies on both payables and receivables. Enforce transaction dollar and volume limits. Establish eligibility requirements to utilize the service.

Approaches for Mitigating Fraud

What follows is a list of technical and behavioral controls for fraud mitigation including both behavioral/process practices which focus on activities a consumer or organization can undertake as well as technology tools which can be implemented. Many of the approaches apply equally to all digital channels, mobile, and web. Mobile devices including tablets and smartphones have become a very common platform for Faster Payments. Their mobility and size make them a favorite of many over PCs and laptops, but those advantages carry with them disadvantages as well. For example, you are far more likely to lose your smartphone or have it stolen than for the same to happen to your PC. Fortunately, mobile devices and PCs have mechanisms that, when properly implemented, can mitigate the unique risks they carry.

Behavioral/Process Controls

There is no substitute for how you, as a person, engage in your own security. Customer and employee education is important and these are the topics that need to be addressed. Some of these behaviors are

fully dependent on the actions of an end-user. Others can be enforced through policies and procedures. Below are important behavioral/process actions which can protect customers' money from bad actors and fraudsters.

Do not write down passwords and place on the screen, under the keyboard, or in a drawer. Just like you would not tape your house key to the front door, do not write down your password and keep it by your computer. Train your mind to think in secure passphrases or, if you absolutely must, type your passwords in a secure document or password management application, understanding that these applications are also vulnerable to risk. **Ensure that the password used to access this cache is used nowhere else.** That way, you only have to remember one password or passphrase. If your system will allow it, using biometrics like facial and thumbprint recognition significantly reduces friction and allows easier, yet secure, access to your computer without the use of passwords. The purpose of security is not to frustrate you, but to enable you to protect what is yours.

Lock your device when you are finished or enable auto-lock.

Use Anomaly Detection using Artificial Intelligence or Machine Learning to detect potentially fraudulent activity. Many payment providers use Artificial Intelligence (AI) or Machine Learning (ML) to analyze behavior and raise an alert if activity on your account does not adhere to expected behavior. It is a good idea to check with your provider and ask about the parameters of how this operates. For example, if you are traveling to another country and you are taking your laptop with you, a different IP address may cause issues with you being able to access the system. Letting your provider know ahead of time can save you trouble while abroad.

Double-check recipient and transactional information prior to executing a payment. Always remember: Computers do what you *tell* them to do, not what you *want* them to do! Best practices recommend double- and triple-checking recipient information prior to sending funds via any mechanism, especially via Faster Payments. Whether you use Faster Payments through mobile or stationary devices, ensuring that the entity (person or organization) receiving the money is correct and is paramount; verify the accuracy of the recipient to ensure the funds are transmitted as intended.

Use Transaction Limits if available. While many providers have a set dollar amount as a default, they will work with you to raise or lower a limit that is in alignment with your typical transactions.

Close or Exit Banking and Faster Payments Applications when not in use. Since your smartphone can be lost or stolen in seconds, train yourself to manually lock it and exit Banking and Faster Payments apps that involve your money and privacy. If your phone is stolen, this added layer of protection will aid in preserving security of your applications.

Business Email Compromise (BEC) is a popular method used by fraudsters to infiltrate an organization's financial systems. Controls specific to helping to mitigate BEC events are as follows:

- Provide education to all parties involved in the payment flow, from the consumer or end-user authorizing a payment, to the organization processing the payment, to their partner financial institution who will execute the payment based on the payment instructions. They should be reminded:
    - Not to respond to or open attachments received in unsolicited correspondence

    - Be wary of pop-up messages or other alerts indicating their computer or phone is infected which can be remediated by clicking a link[31]
- Setting policies for providing appropriate verification of any changes to existing invoices, bank deposit details, and contact information
- Instituting strong internal controls that prohibit payments initiation based on emails and other less secure messaging systems
- Using a two-step verification process that includes contacting the requestor using contact information already on file for them. Confirming requests for transfer of funds or change to payment information by calling the authorized contact at the payee organization using a phone number from a system of record (not numbers listed in an email)
- Monitoring payment history for known vendors and customers to identify requests that do not align with normal activity
- Adopting at least a two-factor authentication and other added layers of security for access to company network and payment initiation
- Email rules that flag emails where the "reply" email address is different than the "from" email address shown
- Visually marking emails with text or color to indicate that they are external emails or modifying the subject line

Technical Controls

Login Authentication

Behavioral Biometrics: Existing protections are augmented by enabling physical biometric security features, such as fingerprint or facial recognition. Behavioral Biometrics add a human dimension to authentication and may be employed to continuously evaluate the authenticity of an established session, which can help thwart fraudsters using stolen credentials as well as identify bots. These enhanced security features scrutinize behaviors like how a user holds a device, types, and moves the mouse, as well as evaluate audit logs to detect behavioral anomalies.[32]

Physical Biometric Authentication: Use of a fingerprint reader or facial recognition with your PC, laptop or PC/Tablet (like the Microsoft Surface), or mobile device is a secure way to access your system without having to remember passwords. These mechanisms are not always available, resulting in passwords continuing to be a standard method of authentication.

Anomaly Detection/AI to detect potentially fraudulent activity. Check with your provider to see what types of security practices they are using to protect you and your money, and controls you can take advantage of.

Complex passwords should be used for access to all systems including Faster Payments. The National Institute of Standards and Technology (NIST) recommends that passwords should be randomly generated, at least eight characters or longer, and up to 64 characters with a combination of numbers, upper- and lower-case letters, and symbols. It also recommends against password reuse, that passwords should be verified against known password dictionaries, the use of password managers, at

[31] Fraud Advisory for Businesses: Corporate Account Take Over, Nacha, 2019
[32] Behavioral Biometrics for Human Identification: Intelligent Applications, Wang and Geng, 2010

least 10 password attempts before lockout, infrequent password changes, and against the use of words, pets, people, places, and adjacent keyboard strings.[33]

Multi-Factor Authentication (MFA) requires two out of three types of credentials for authentication: something you know (such as a password), something you have (such as a phone), or something you are (such as a biometric). Most MFA mechanisms consist of a 5-6 digit numeric value that is sent via SMS, push notification, or email. Since the message is on a different channel – the cell phone network vs. the Internet – it is considered Out-of-Band-Authentication (OOBA), a deterrent to fraudsters. The idea behind OOBA is that two physically separated devices will authenticate a single transaction. The probability of a hacker having access to both your PC and your mobile phone at the same time is lower.

Knowledge-Based Authentication (KBA): KBA authenticates end-users by asking "shared secret" questions which only the actual person should know. Typically, the answers are "out-of-wallet," meaning that the information to answer the question is not available in a person's physical wallet. NIST[34] specifies that KBA does "not constitute an acceptable secret for digital authentication" in multi-factor authentication since it is easily compromised. Though some systems allow customers to make up their own questions to be used and stored, making the answers harder to guess, anything known is potentially at risk of being inadvertently shared or stolen, thus KBA is vulnerable to numerous compromise methods.

Device Identification: Many financial institutions will use a "smart cookie" to identify your device as having previously authenticated with their Faster Payments system. If the website you are using says, "Remember Me on This Device," and you click the check box, it is likely their system shares and stores information on your PC via internet cookies. The next time you visit the site, if the smart cookie is there, the system probably will not ask you "out-of-wallet" questions. You should never enable a smart cookie on a public device or a PC you share with others. The few seconds this saves is not worth the security risk. With a smart cookie enabled, only a username and password are required to access the system.

Inactivity Locking and Logoff: It is best practice to lock your computer when you are not using it. Because we all get busy and forget, enabling "Auto-Lock" is an easy way to protect access to your computer or electronic device. This is a setting that can be enabled to make you enter your password again after a period of inactivity. You can select how much time passes before the system locks. The shorter the time, the more secure your system will be, ranging from seconds to minutes.

Enable "Find My Device": Some people hesitate to enable "Find My Device" features due to concerns of a network operator or some other entity (i.e., "Big Brother") tracking their movements. However, from a practical standpoint, this feature is extremely helpful in locating a lost device. By enabling this feature, you will be able to quickly ascertain whether your device has been stolen or if it is just misplaced. If it is the former, you will have advance notice to contact your financial institution and have them disable your Faster Payments account. If it is misplaced, this will help you more quickly retrieve your device thus saving time, money, and stress.

Transaction Monitoring

Transactional Fraud Detection Using AI and ML: In addition to securing devices used to access a payment system, financial institutions, organizations, and consumers are advised to enable fraud

[33] Top Ten 2019 Password Security Standards, Liquid Web, 2019
[34] NIST Special Publication 800-63-3: Digital Identity Guidelines, NIST, US Department of Commerce, 2017

detection at the transaction level. ML uses a set of established rules and continually updates its data set to "learn" about authorized and fraudulent transactions. This output is used to update the rules and identify new trends. AI acts more like a human and learns new concepts. The technology can constantly analyze user interactions, transactions, and payment behaviors; consider economic factors; and identify suspicious transactions. Using AI, each account has its own, unique profile as opposed to applying a standard ruleset to a group of accounts.[35]

Text and Email Notifications of transfers, failed login attempts: Many financial institutions offer notifications of activity on your account. Enrolling in text alerts and email notifications will inform you of activity or attempted activity on your account. For example, a text message will inform you every time a Faster Payment has completed. If you did not initiate it, you will know quickly and can contact your financial institution and turn off your card or lock down your account. Additionally, an email message every time a password is mistyped can alert you if someone is trying to gain access your account. As unnerving as these events can be, they are far preferable to discovering fraudulent transactions long after they have occurred. As the saying goes, "Forewarned is Forearmed."

Account Tokenization and Validation

Tokenization or **aliases in a directory** can be applied to mask banking credentials. The accountholder's account number at the financial institution is substituted with either a token, or associated with an email address or telephone number.

Account Validation and Verification Services provide originators and requestors of payments insight to the status of the counterparty account to determine if it is open, closed, or in a negative status, and simultaneously or separately validate that the counterparty name (consumer or business) is authorized to transact on the account. These services complement many payment methods or act as a standalone service, aid in compliance with Nacha WEB entry SEC code debit rule changes, assist in reducing unauthorized returns and associated fees and losses, and allow customization for increased fraud prevention coupled with reduced friction and in a near-instantaneous experience prior to processing.

System Security Controls

Due Diligence: Faster Payment operators should perform due diligence on system participants to form a reasonable belief the participant can meet security and protection of PII requirements. Financial institutions should implement a risk management program to comply with these requirements.

Anti-Virus/Anti-Malware programs have been around for years and provide protection against viruses. It is important to understand that even in a best-case scenarios, they cannot protect against every cyber-threat. Still, it is important to have these programs running and configured to automatically download updated virus definitions on a daily basis at minimum. Regular scans of your computer's memory and hard drives are important, too. Most Anti-Virus and Anti-Malware programs are automatically configured to do this, but it is important to confirm your subscription is current. The cost of this protection is relatively low, especially in comparison to the cost of a bad actor or fraudster gaining access to your computer and initiating fraudulent Faster Payments transactions.

[35] How FIs Are Using Artificial Intelligence And Machine Learning, PYMNTS.com, 2019

System Hardening: Almost every new PC comes with pre-loaded software that you may never use. It is important to uninstall programs you are not going to use. This must be done with caution since some seemingly unused programs actually complete important tasks like run your video and sound cards. If you are uncertain of which programs are unnecessary, consult with an IT professional before uninstalling them.

Automated Patching: Computer programs, be they operating systems like Microsoft Windows, Linux or Apple's Sierra; web browsers like Apple Safari or Google Chrome; or ancillary programs like Adobe Acrobat or Java include vulnerabilities. As a result, "patches" to fix discovered vulnerabilities are pushed out to computers running said programs on a regular basis. Most programs are now set to automatically update, occasionally requesting permission before doing so. It is easy to ignore these prompts and tell yourself you will get to it later. However, almost all exploits hackers use to gain access to your computer take advantage of known vulnerabilities on unpatched programs. Therefore, it is very important to keep your system up-to-date, and test these patches whenever possible to ensure they do not cause additional issues on other systems.

Enable Auto-Update of applications and operating systems of mobile devices. Just like with PCs and laptops, operating systems of mobile devices receive updates to add features and patch security vulnerabilities. The same is true of the apps you have downloaded. Fortunately, most mobile devices allow and promote the auto-update of both the operating system and apps automatically. It is easier to keep your smartphone and all your apps up-to-date than to do the same for your PC or laptop. With just a few taps, you can be sure your phone or tablet has the latest software available.

Electronic Consent-Based Social Security Number Verification (eCBSV) is an electronic modification of the paper-based process, and provides responses in real-time, or next to real-time, allowing banks to use the service during account opening as opposed to after the fact.

Education and Awareness

There are many resources available for all types of organizations that help provide or develop education material to bring awareness to current fraud threats and trends, as well as best practices to mitigate the risk associated with these threats. Financial institutions of all sizes can connect with their Payments Association by visiting the Center for Payments. Nacha has compiled a listing of resources related to current fraud threats. Additionally, the FBI has outlined the most common scams and crimes as well as tips to prevent further victimization. A good example of a consumer education campaign from the United Kingdom is "Take Five to Fight Fraud."[36]

Figure 2: UK FasterPayments.org Consumer Education Campaign

[36] Take Five to Fight Fraud, Fasterpayments.org.uk

Summary and Conclusions

Faster Payments promise to provide untold benefits for a vast array of users as the U.S. payments ecosystem continues to modernize and change dramatically. The FPC is an inclusive membership organization that is devoted to advancing Faster Payments in the United States. By bringing all the industry's stakeholder segments together, the FPC is driving the Faster Payments ecosystem to evolve in a manner that supports competition and is open, fair, flexible, and responsive. The FPC's mission means it is the one industry organization to tackle topics such as interoperability, the regulatory environment, and Faster Payments fraud prevention. FPC work groups initiate industry action by developing tools, guidance, and other resources to push toward the future of Faster Payments for all.

Fraud is not new to the payments landscape and with the introduction of a new Faster Payments channel, we can expect fraudsters to do what they do best — exploit and manipulate any weaknesses in the ecosystem. Since these new payment systems are becoming more ubiquitous, two of the most important actions one can undertake is to become aware of the fraud trends and themes, and find ways to mitigate them. In this white paper, the Fraud Information Sharing Work Group has done just that. The Work Group has provided insight into common fraud themes impacting Faster Payments and best practices and strategies to help you design the mitigation strategies that will be most effective for you and your organization.

Some tips to protect your organization:

1. **Conduct an independent assessment** – Engage an experienced engineering firm that understands the technical risks and complexities of enterprise architecture to do a complete technical independent assessment of your firm's infrastructure. Make sure to engage a company that has more technical expertise than a general consulting firm. You should know where your vulnerabilities are at all times and address them accordingly.
2. **Engage government and law enforcement** – Ensure you have a clear engagement model with the government, including law enforcement. Who are you going to call? Which agency, and under what circumstances? Have the relationship established up front and the engagement documented in a run book.
3. **Join FS-ISAC** – Join an industry-based sharing forum. If you are not already part of FS-ISAC, we encourage you to join.
4. **Simulate an internal attack** – Create a Red Team and have them attack your systems using the same techniques bad actors and fraudsters employ. Not once a year, all the time. Also consider establishing a program to harvest credentials and account numbers that might be in the underground related to your bank to detect compromises you may not otherwise be aware of.
5. **Deploy mandatory employee training and testing** – Malicious email is one of the most prevalent ways bad actors and fraudsters penetrate organizations. Establish a baseline training program for all employees that is mandatory and focuses on the specific actions employees need to take to protect the firm. Once you have trained your employees, actively test them. For example, start sending your employees targeted phishing that requires those who click in the phishing emails to take additional training.
6. **Know your third-party vendors** – Understand your third-party environment and upgrade your contract provisions and ensure they are following the same standards you are striving for in your own environments. Vendor Management can be overwhelming, especially for smaller institutions and businesses. Focus attention on those vendors that have direct access to customer and

transactional data. Request and review independent audits of these companies to ensure their practices are at least as strong as yours. For additional details, consider the FFIEC Guidance on Vendor Management.[37]

7. **Exercises and drills** – Run simulations and drills to assess your capability. Use a combination of scenario exercises and live inject of events into your Security Operations Centers to see how it responds. Learn lessons and repeat. Include colleagues from the business in addition to technologists in the table top exercises.
8. **Know how money leaves and enters the organization** – Look at all of the ways money moves in and out of your institution. Identify what controls and thresholds you can implement to protect money movement, assuming bad actors and fraudsters circumvent your other controls. Examples: wire limits, country destinations, and new beneficiaries.
9. **Implement controls for maximum effect** – Using your web filtering software, block category "None"—a hugely important mitigation technique. Leverage technology called DMARC. This allows you to ensure that others have a way to validate that emails that appear they are originating from you, are actually coming from you.
10. **Protect your computers** – Consider physical and logical network segmentation for funds transfer related computers; employ the concept of 'least privilege" to limit the use of administrator privileges; and consider limiting the processes and services that can be run on for funds transfer related computers (e.g., no email or restricted use for Internet browser applications).

FPC Fraud Information Sharing Work Group Members:

Andrew Haskell – BNY Mellon (Chair)
Deborah Baxley – PayGility Advisors LLC
Elspeth Bloodgood – Jack Henry
Richard Bradfute – James Polk Stone Community Bank
Ryan Dutton – SHAZAM
Chris Garcia – Commerce Bank
Tanya Hughes – Navigant Consulting, Inc.
Rakesh Korpal – JPMorgan Chase
Rebecca Kruse – ICBA Bancard
Neil Kumar – Alloya Corporate FCU
Jason Paguandas – Visa
Beatriz Saldivar – Axletree
Shoaib Shafquat – QCheque
Peter Tapling – PTap Advisory, LLC
Michael Timoney – Federal Reserve Bank
Eric Wester – Upper Midwest ACH Association

[37] IT Examination Handbook, FFIEC