THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

REMOTE AUTHENTICATION
FRAUD LANDSCAPE SERIES
AUGUST 2021

BRIEF #2:

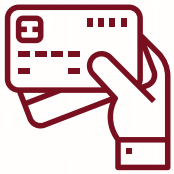
Fraud Types and Authentication for Remote Payment Use Cases

OVERVIEW

This is the second research brief in our series on remote authentication fraud,[1] which is defined as fraud that occurs when someone who is not the legitimate owner of an identity or financial account either creates a new account or takes over an existing digital account for the sole purpose of committing an illegal activity using stolen payment credentials or unauthorized payment information. Authentication fraud can occur when the legitimate owner conducts a digital financial activity, i.e., via a mobile phone app, mobile browser or PC internet browser, to:

Open a bank account or credit card through mobile or online banking

Enroll a bank account or credit card with a third-party payment provider or proprietary merchant contactless mobile or digital wallet



Initiate a payment transaction from a digital wallet

Enroll in a person-to-person (P2P) payment service or initiate a P2P funds transfer

In all cases, the customer is not present physically at the financial institution or merchant point of sale (POS).

Authentication of the customer and payment method needs to occur at each step in the remote payment process: account creation, enrollment and transaction – to identify, prevent and mitigate fraud attacks.

1 Remote Authentication Landscape and Authentication Methods. July 2021

Types of Authentication Fraud

New account fraud (NAF) and account takeover (ATO) are the primary methods that fraudsters use to open new accounts or access existing financial accounts to steal customer funds or charge purchases using newly created or stolen payment credentials.

New Account Fraud (NAF)[2]

New account fraud targets multiple payment accounts via mobile or digital channels, including demand deposit accounts (DDAs), credit cards, online/card not present (CNP) merchant or third-party accounts. Fraudsters open accounts individually or use automated scripts to execute NAF attacks that can target multiple institutions simultaneously by hijacking a computer and attempting to open hundreds of accounts in a short amount of time. They often use the same device repeatedly to perform fraudulent transactions until the device is detected and access can be disabled.

Larger, more sophisticated financial institutions (FIs) use device recognition and behavioral tools to block malicious traffic, but less sophisticated or smaller organizations may be more vulnerable if they rely heavily on personally identifiable information (PII) for identity validation.

NAF based on stolen legitimate identities

Fraudsters use identity data sourced from data breaches, phishing or hacking to open new accounts in their victims' names. They pretend to be people whose identities they have stolen to:

(1) circumvent authentication,

(2) intercept communications from FIs and

(3) establish temporary deposit and withdrawal patterns intended to convince the financial institution they are the legitimate account holders.

Once fraudsters have gained trust, they can perform any function the financial institution offers its customers, including applying for loans, increasing credit limits, making purchases, transferring or withdrawing funds and generating fraudulent checks. FIs may attempt to recover the funds from the victims but have no recourse when customers were unaware of the fraud.

Once fraudsters have gained trust, they can perform any function the financial institution offers its customers.

2 NAF also is known as account opening fraud or online account origination fraud.

NAF based on Synthetic Identity Fraud (SIF)

Perpetrators use a combination of PII to fabricate a person or entity in order to commit a dishonest act for personal or financial gain. Their methods include:

- Identity fabrication (completely fictitious identity without any real PII)
- Identity manipulation (using slightly modified real PII to create a new identity)
- Identity compilation (combination of real and fabricated PII, such as a false driver's license, a real shipping address and phone number, and false name and date of birth)

Once a synthetic identity is established, the synthetic identity holder will begin to build credit by applying for a credit card or bank account – and eventually, after bypassing the FI's ID&V (identity and verification) process[3] and creating a password and username for online transactions, use the new credit card or bank account to commit payments fraud. What differentiates SIF from other types of identity fraud is that the fraudster can build a credit score over months or years, which provides the appearance of legitimacy.

Because synthetic identities often pass traditional verification processes, financial service providers struggle to detect the fraud, which can lead to significant losses[4] and further underlines the impotence of legacy identity-proofing approaches. In 2020, identity-based fraud remained a top factor for fraud losses. While the overall percentage of reported identity-based fraud was similar to the previous period, the amount linked to synthetic identity fraud has increased, with synthetic identity fraud growing among mid-size/large firms and those using the mobile channel.[5]

Account Takeover (ATO)

Account takeover fraud occurs when fraudsters use card or bank account credentials, username and passwords and/or PII (e.g., email address, name and date of birth) to gain access to a legitimate bank, payment service provider (PSP) or merchant customer's account that is stored on file by the merchant.

ATO attacks can happen in a variety of ways. Some ATO attacks begin with fraudsters harvesting personal data,[6] which can occur long before a fraudulent transaction takes place. Fraudsters use the harvested data to prepare targeted phishing campaigns. They also may gain unauthorized access to accounts by using an automated attack or manually typing in combinations of credentials. If the FI's authentication mechanisms rely on weak security measures, such as static passwords, fraudsters may use a

3 The identity and verification (ID&V) process verifies the previously established identity of the account holder or cardholder. Verification answers the question, "Is this person who they say they are?" For mobile or digital payments that are tokenized, ID&V ensures that the legitimate cardholder is using the payment token associated with the Payment Account Number (PAN). FIs may use biometrics, machine learning (ML) data or passwords to complete ID&V for remote activity.

4 The top 5 issuing banks have seen $5+ billion in losses linked to synthetic identity fraud, according to IDC Financial Insights. Fraud strategy has a new role: enabler of innovation. March 2020.

5 2020 True Cost of Fraud™ Study. July 2020

6 Data harvesting is a process to extract large amounts of data from websites automatically using bots. The technique is often used without permission to steal website and database information, such as contact lists, email addresses and other PII.

technique known as credential stuffing, which occurs when a large number of bots (automated software that runs per instructions without human intervention)[7] compare lists of stolen credentials against a range of websites to find a match.

Once fraudsters have access to an account, they can alter customer account details, including address, email and phone numbers. They can change the password to lock out the account owner, add another name and redirect account change notifications, fraud alerts and other FI communications to the fraudster. Fraudsters can add their own voice recognition to the account, which is another way to lock out the legitimate customer. Most FIs do not have effective controls to detect this type of activity once the fraudster has access to an account.

Until recently, FIs and card providers were the main targets of ATO. However, as EMV chip cards replaced magstripe cards to improve physical credit card security, it became more difficult for fraudsters to use stolen or counterfeit cards at point-of-sale (POS) locations. At the same time, more customers were transacting with e-commerce businesses that offered a user account or membership, making those online retail accounts more attractive to fraudsters using stolen credentials.

Account takeover is becoming a leading form of fraud for online payments.

Account takeover is becoming a leading form of fraud for online payments. SIFT reported that ATO fraud attempts to steal from consumers and e-commerce merchants grew 282% between Q2 2019 to Q2 2020.[8] This can have serious consequences, as FIS Global predicts mobile commerce[9] sales will grow at 19% on average to reach $2.29 trillion by 2022, while estimating that physical sales will grow at less than 5% annually over the same period.[10]

Already, financial services firms are seeing a 42% increase in successful monthly fraud attempts compared to 2019,[11] and a 2020 industry survey of merchants reported that 35% of respondents had ATO rates of at least 10% in the previous year.[12]

7 A bot (short for robot) is automated software that runs per instructions without human intervention. Bots usually operate over a network. They often imitate or replace a human user's behavior and can perform repetitive tasks much faster than humans. "Bad" bots are programmed to break into user accounts, scan the web for contact information for sending spam, or perform other malicious activities. A botnet is a large network of bots, or collection of internet-connected devices infected by malware. Cybercriminals instigate botnet attacks (e.g., identity theft or ATO, credential leaks, unauthorized access, data theft or distributed denial of service/DDos attacks), leveraging huge lists of stolen credentials. Once in, they can use real accounts, along with saved credit card information, to buy products either from the account itself or through credit card skimming. What is a Bot?

8 Digital Trust & Safety Index: Content Abuse and the Fraud Economy

9 Mobile commerce is a form of e-commerce, initiating a remote or online purchase from a mobile phone app or mobile browser.

10 Preventing Account Takeover – is there a better way? May 2020.

11 2020 True Cost of Fraud™ Study. July 2020

12 Payments Journal, "Merchants are unprepared to tackle threat of ATOs." July 2, 2020. Riskified surveyed 4,000 customers and 425 merchants.

Account takeover fraud can have consequences for all aspects of business, from profits and productivity to customer loyalty and growth. Using strong authentication tools and rules for digital payments, providers and merchants can quickly analyze other activities and transactions that are typically out of pattern to determine potential risks, including:

- Same items being purchased multiple times
- Device and network data, e.g., internet protocol (IP) address, geolocation, etc.
- Proxy usage to determine if the fraudster appears to be in the same geographic area where the account originated
- Previous or unusual formatting in logins to determine if the person accessing the account is the legitimate account holder or a bot
- Anomalous or atypical transactions

Vulnerabilities and Enablers of Remote Authentication Fraud

While the purpose of authentication is to verify a customer when enrolling in an account or making a payment, environmental vulnerabilities weaken the effectiveness of current authentication methods and create new opportunities for fraud. This section describes vulnerabilities associated with authentication and enablers of fraud that can help bad actors bypass the authentication process, gain access to accounts and perpetrate fraud.

Vulnerabilities:

- Increased number of payment-enabled connections or devices and online points to attack
- Increased access to PII data via data breaches, social media oversharing and phishing
- Increased use of email addresses as usernames. An email address does not guarantee the applicant is the legitimate holder of that email address, or even if the applicant is a real person
- Increased number of attributes available for authentication, e.g., email address, mobile number, geolocation and device properties. These changes make authentication routines more complex
- Increased number of devices and channels to access customer accounts and enroll payment account information

- Increased card-not-present (CNP) and other remote transaction volumes, and weaker authentication methods used by some merchants and third parties, particularly smaller e-commerce businesses
- Reduced connection between a user's mobile phone number and geographic address, which makes it more difficult for mobile network operators (MNOs) to verify phone ownership. Because MNOs are not required to comply with Know Your Customer (KYC) and other financial service guidelines, they may not follow consistent practices to validate a customer's identity, enabling fraudsters to take advantage of stolen phone numbers.

Personally identifiable information is more readily available to fraudsters due to data breaches, social media oversharing and phishing.

Fraud Enablers:

Data Breaches

A data breach exposes confidential or protected information, potentially resulting in the loss or theft of an individual's SSN, bank account or credit card credentials, personal health information, usernames, passwords, email addresses or other PII. Fraudsters purchase this information on the dark net[13] to access payment credentials that customers have with FIs, online merchants or PSPs and to create new accounts.

Phishing

Phishing is a form of social engineering that uses email, phone or text to entice individuals into providing personal or sensitive information, ranging from passwords, credit card information and Social Security numbers to details about a person or organization. Attackers pose as legitimate representatives to gain this information, which is then used to access accounts or systems, often leading to identity theft or significant financial loss.[14] They purport to be from trustworthy entities to induce the receiver to reveal confidential information.

Spear phishing[15] narrowly targets *specific* individuals or organizations by sending emails that appear to be from a known sender (e.g., a bank or third party with whom the individual may have a relationship) to induce the receiver to reveal confidential information. Spear phishing campaigns tend to be more elaborate and customized to their intended target.

13 The dark net refers to websites that are specifically used for nefarious reasons. Dark net sites are purposefully hidden from the surface net and facilitate black markets, e.g., illegal file sharing, exchange of illegal goods or services, including stolen financial and private data. Most dark net websites use encryption to help hide their identity. What Is the Dark Net? January 2020.

14 What Is Phishing? A Brief Guide to Recognizing and Thwarting Phishing Attacks

15 Spear phishing

Phishing often directs users to enter PII at a fake website, which looks like the legitimate site. Fraudsters gain access to sensitive information and account credentials to perform financial activities, including, but not limited to:

- Enrolling a stolen card or bank account with a PSP or merchant to make purchases
- Enrolling stolen credentials in a new P2P account (NAF) to potentially transfer funds to the fraudster's account
- Using stolen credentials to access an existing PSP, merchant or P2P account (ATO).

Fraudsters prey upon people by creating a sense of urgency or exploiting their trust in established institutions. A phishing email from the recipient's FI may look like a valid communication alerting the user that his or her account is at risk. It also may contain links or attachments that appear to be documents from the FI or include other details of a legitimate email, such as logos, email signatures and real employee names.

Phishing emails trick customers into transferring funds or sharing their credentials by:

- Clicking on a link that redirects them to a fake website
- Entering their usernames and passwords to access a compromised website
- Opening an email attachment that installs malware on a device to intercept their banking credentials the next time customers enter them into the bank's legitimate site
- Prompting customers to call a number where the receiver is a well-trained fraudster impersonating a bank representative; or convincing customers to share a one-time passcode (OTP) with the fraudster who initiated the request to get into customers' digital accounts.

Malware

Malware, short for malicious software, is an umbrella term that refers to several forms of intrusive software. Malware compromises computer functions to steal data, bypass access controls and cause harm to host computers, customer devices and their applications or data. Malware infects cardholder devices/wallets to access sensitive information, such as passwords, and payment credentials that can be captured when victims enter data into an infected device.

Users inadvertently install malware on their computers or mobile devices through a wide range of actions. These include visiting unfamiliar websites (that often appear legitimate), opening attachments from phishing emails or downloading mobile apps from untrusted sources. Malware programs can perform different kinds of attacks. Some install configuration files on the infected device to redirect the victim to a malicious website that can expose information on the device or harm the device itself.

Trojans are a type of malware often disguised as legitimate software that use overlay attacks to steal login credentials and payment card details from users of online and mobile banking applications. The overlay attack creates an additional layer on top of the user interface on the mobile device. Once it detects that the online/mobile banking app is running, it will activate, push the targeted app to the background, and display its own login interface instead. When the victim authenticates, the Trojan malware collects the user's credentials. Mobile banking Trojans can remain active and modify the data while the victim performs other actions within the banking session.

Man-in-the-Middle (MitM) and Man-in-the Browser (MitB)

These attacks are commonly used with, or initiated by, malware. MitM attacks intercept a communication between the customer and the FI and then alter, send and receive communications about the transaction details without raising suspicion. They can affect the mobile banking channel when customers use unsecure public hotspots to log in, authenticate and/or transfer payment data through a network controlled by the fraudster, who is able to gain access to usernames and passwords that are stolen during transmission. A MitB attack is a form of session hijacking[16] that infects a web browser by installing an add-on to intercept credentials or modify transaction details.

When MitM/MitB and malware are combined, these attacks create widespread disruption. Malware disrupts the mobile device operating system to steal Payment Account Numbers (PANs) and PII, which the fraudster then uses to create accounts with online/mobile merchants or PSPs. When combined with MitB or MitM, the malware infects the account with code that the fraudster controls. This enables the fraudster to perform various activities, such as intercepting future banking or purchase transactions, redirecting money transfers, or intercepting a text message to capture a one-time passcode and redirect the transaction data.

Sim Swap Attacks

A subscriber identity module (SIM card) is an integrated circuit that securely stores the international mobile subscriber identity number and its related key, which authenticating parties use to identify and authenticate subscribers on mobile devices.

SIM swapping[17] attacks occur when fraudsters take advantage of a weakness in two-factor authentication and verification. Fraudsters impersonate legitimate customers of the mobile carrier to deactivate a victim's SIM card and obtain a new card with the user's phone number and data, which can give them access to financial account information. Fraudsters impersonate customers using social engineering to yield enough PII to answer security questions or provide account verification details.

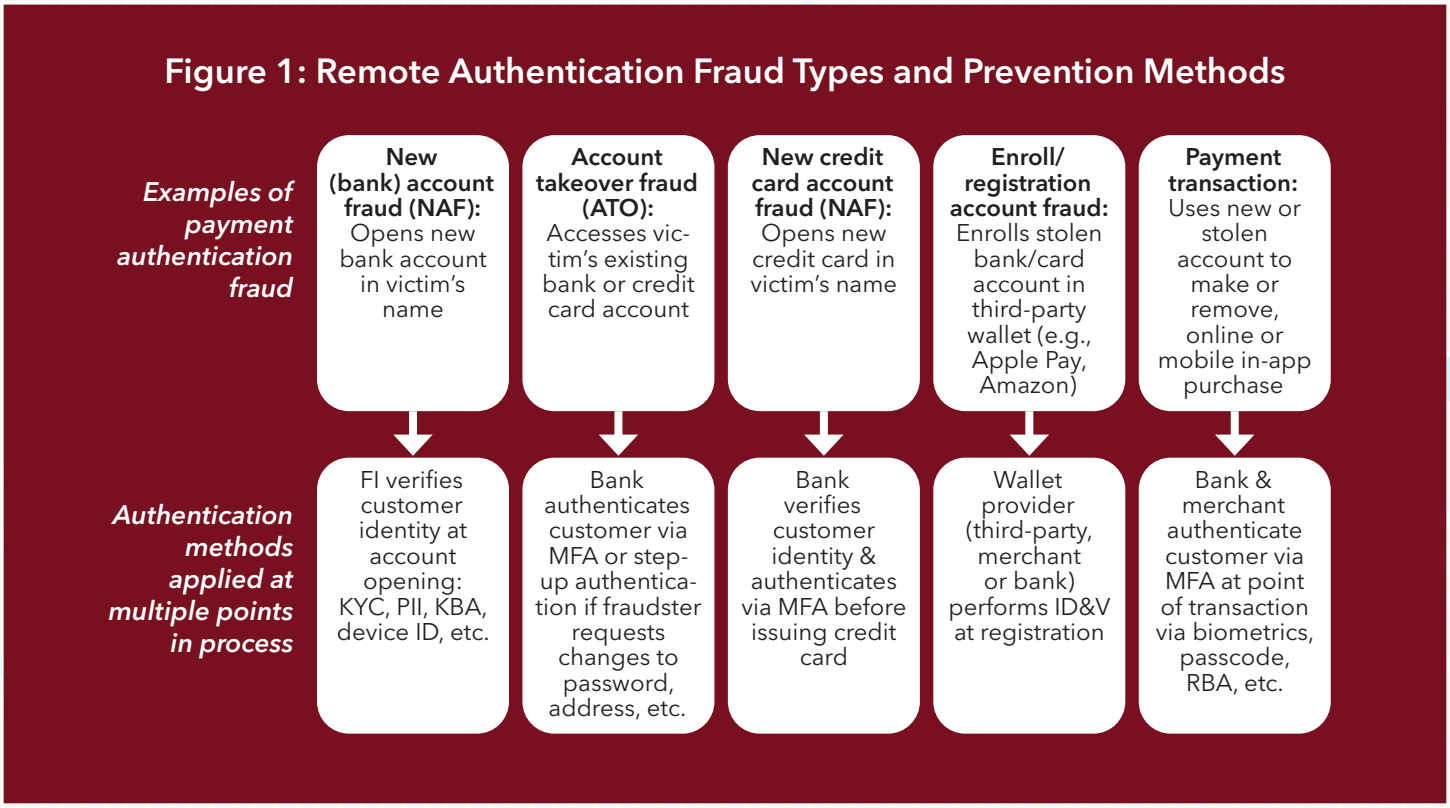
Fraudsters then target online banking services that use mobile phones in the authentication flow. For example, if enrollment of a mobile banking app happens via

16 Session hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID. Session hijacking involves an attacker using captured, brute-forced or reverse-engineered session IDs to seize control of a legitimate user's Web application session while that session is still in progress. Session Hijacking. May 2021.

17 SIM swap fraud explained and how to help protect yourself, November 8, 2019.

the SMS (short message service)[18] channel, SIM swapping may enable a fraudster to activate the app on his or her phone. If the bank's authentication mechanism uses text messages to deliver OTPs, the fraudster can take over the victim's phone number to authenticate fraudulent transactions or perform other operations in a customer's online banking session.

Figure 1: Remote Authentication Fraud Types and Prevention Methods



Authentication for Remote Payment Use Cases

The customer journey begins by digitally opening, verifying and authenticating a new Demand Deposit Account (DDA) or credit card account. Customers can then enroll their financial accounts with online merchants, enroll with a PSP or mobile/digital wallet and purchase goods and services, and/or enroll and transfer funds via a P2P mobile app.[19] Which authentication methods are used will vary depending on the stakeholder risk analysis, the specific use case and payment method, at a minimum, along with many other variables.[20] These use cases assume that the fraudster has the victim's PII, password, bank or card credentials prior to an attack and is able to take over an existing account (ATO) or create a new account (NAF). Because fraudsters can attack at various points, authentication should occur at multiple steps in the enrollment and transaction process.

18 Short message service (SMS) is part of the GSM standard that enables a mobile device to send, receive and display messages of up to 160 characters. Messages received are stored in the network if the subscriber device is inactive and are relayed when it becomes active. SMS has become available increasingly in CDMA networks and in some fixed networks. Definition of Short Message Service (SMS)

19 Examples of PSPs: PayPal, Amazon; mobile wallets: Apple, Google, Samsung Pay; P2P: Zelle, Venmo, Square Cash.

20 These use cases will be described in more detail later in this brief and cover vulnerabilities and potential risk mitigation tools.

USE CASES

NEW ACCOUNT OPENING and ONBOARDING of BANK DDA or CREDIT CARD ACCOUNT

New account opening applies to the remote opening of a demand deposit bank account and associated debit card and/or credit card. When applying for a new account, a customer accesses the website or downloads the mobile app of the depositary or credit card-issuing financial institution.

Know Your Customer

FIs deploy mandatory KYC compliance to verify the identities of their customers and perform due diligence to prevent fraud and money laundering. At a minimum, the FI must obtain the following identifying information from each customer before opening a deposit or credit card account in person or remotely:[21]

- Name, date of birth, address, identification number (SSN or Taxpayer Identity Number (TIN))
- *Documentary evidence* of a customer's nationality or residence with a photo or similar safeguard. Examples include a driver's license or passport, which a customer can submit electronically by scanning or taking a picture.
- *Fraud protection information* that the applicant must provide, e.g., mobile phone number, email and mother's maiden name.

Identity Proofing

To validate the customer's identity, the FI may use a vendor identity verification (IDV) solution, credit bureaus and/or point solutions, including device verification, biometric capture, document verification, mobile number and email. When approved, customers create a username and password and select several knowledge-based authentication (KBA) security questions and answers that serve as an authentication for password resets and multi-factor authentication (MFA). Customers receive an OTP via email or SMS text to confirm their account opening.

Of U.S. financial institutions surveyed in 2019, 85% have experienced fraud in their digital account opening process.

21 Customer Identification Programs

Thirty-five percent of U.S. financial institutions surveyed by a computer security firm in 2019 said that opening new accounts digitally is a top priority because they are losing customers who are giving their business to other banks and lenders that offer this ability. Priorities for these institutions include streamlining the digital onboarding process for new applicants (80% of respondents). However, 85% of all respondents have experienced fraud in their digital account opening process and more than 50% of respondents continue to have security or fraud incidents because of their digital account opening application process.[22]

Vulnerabilities associated with New Account Opening

Ineffectiveness of Customer Identification Programs (CIPs)

A CIP program alone cannot effectively detect and prevent financial crimes. Criminals can easily fabricate forged documents, which they combine with name, date of birth and address information bought on the dark net. Not all fraud departments have sufficiently trained or experienced staff to keep up with increasingly more complex and sophisticated ID documents that are submitted digitally through remote applications (online or mobile). The risk of identity compromise also increases because there is no physical connection between the applicant and FI employee.[23] While some industry experts suggest not relying on CIP as a FI's sole method of identity verification,[24] it meets many of the existing regulatory requirements such as KYC, where auditable results are required to demonstrate compliance.

Compromised data sources

Credit bureaus have had difficulty detecting both synthetic identity fraud and identity theft. It may be more difficult for credit bureaus to corroborate the identity of individuals who lack credit history due to the use of alternative financial services, age or verifiable ID documents of recent immigrants. The 2017 Equifax data breach emphasized that credit bureaus are not immune to hackers, who obtained the PII of 147 million customers in the U.S. and Canada through this single data breach. Because Experian and Transunion also store much of the same customer PII, the breach put them at risk, as well.

Social Security Number (SSN). The original purpose of the unique nine-digit SSN was to track the income of U.S. citizens and eligible U.S. residents and determine government benefits. It has become a de facto national identification number for taxation and other purposes because the U.S. does not have any other national common identifier. While SSNs were never intended or designed to be so widely used to identify or authenticate individuals, they have performed as such for years on a large national scale. Today, SSNs may be used to obtain credit, open a bank account, buy a home or a car, and apply for a passport or driver's license. Because

22 ISMG, OneSpan. "The State of Digital Account Opening Transformation" Survey of 100 primarily U.S. FIs, Fourth Quarter 2019.

23 Some identity/document verification solutions attempt to perform the role of bank staff in the digital world with selfie + document capture. However, solutions still need improvements: they only auto-capture about 25% of the approximately 20 security features embedded in ID docs, so the remainder require manual review. Fraudsters can determine and then focus on those auto-check features. In the physical world, that determination is more difficult, forcing fraudsters to falsify more security features in the physical document.

24 Gartner strongly recommends that security and risk management (SRMs) leaders move away from this method as their sole method of corroborating the identity of individuals.

the SSN is used in so many places, it has made it easy for a fraudster to steal the SSN and use it in combination with other PII to apply for credit, take out loans, get a job or obtain healthcare in the victim's name.[25]

PERSON-to-PERSON (P2P) PAYMENT AUTHENTICATION for ENROLLMENT and TRANSACTION

Person-to-person (P2P) payment services allow digital funds transfers between individuals' accounts without revealing the recipient's financial details, using a mobile app, an online digital solution (e.g., PayPal) or online banking. Newer P2P solutions offer mobile apps that enable transferring money between friends or splitting bills. The mobile and P2P apps included in this use case support U.S. payments only and are FI-, card- or nonbank-centric. Customers register with a specific P2P solution to send and receive money by linking a valid U.S. bank account, debit card or credit card, depending on the solution.

Authentication for P2P enrollment

During enrollment, the customer adds his or her payment method to the P2P mobile app or online browser service. The P2P provider works with the FI account or card issuer to determine if the customer is the legitimate cardholder or bank account owner.

The P2P payment service provider sends the account/card data to the issuing FI for ID&V and to verify the account and device, if applicable. The FI may request step-up authentication if the risk score is high. Once the FI approves the card or bank account, the FI notifies the PSP, which adds the payment method to its Confirmation of Funds (CoF) database for future use and notifies the customer via email or text.

Authentication for P2P transaction

Customer verification systems monitor payments as they occur 24/7, watching for signs of fraud and immediately alerting customers if they see suspicious activity. Using extensive proprietary risk-based authentication (RBA) tools, they can identify a customer and connect that identification to a larger quantity of customer data to understand behavioral patterns. Their analytic tools verify the authenticity of the payment by drawing on extensive histories of interactions with customers to feed into their risk analytics and AI tools/algorithms and perform transaction fraud scoring. They also collect user/device data for customer authentication, such as geolocation, device fingerprint, device ID, IP checks, IP address and velocity, operating system, web browser, previously visited websites, time spent on sites, purchase or payment history.

If sending money via a card, the PSP also may verify the card security code and review customer enrollment attributes or transaction history. However, if any information appears suspicious, the PSP may challenge the sender with an OTP or KBA before sending the money.

25 Social Security Administration. The Story of the Social Security Number

Vulnerabilities

Settlement risk if funds sent in error to receiver: This affects P2P transactions settled over the Automated Clearing House (ACH) network, unlike P2P funds that are sent in real time that give the recipient immediate access to funds. Settlement of funds between sender and recipient banks through ACH may create an unintended settlement risk for the bank that receives the P2P payment because it can take one to three days for that bank to receive the funds. However, if a bank connects to an instant payments network, funds are received immediately and the settlement risk is eliminated.

Customer sends funds to incorrect recipient and has no recourse to recover funds: While this is not an authentication vulnerability, some P2P solution providers ask senders to verify the recipient information before initiating the transaction as part of their authentication strategy.

ENROLLMENT in CONTACTLESS MOBILE and DIGITAL WALLETS

A contactless mobile wallet is a device/OS-centric wallet application that stores payment tokens associated with a credit or debit card PAN and related card/PII data on a mobile device or in the cloud.[26] Each wallet supports the use of device biometrics, and offers the option for the customer to enroll a fingerprint, facial recognition, iris scan or use a passcode/PIN to authenticate when purchasing at POS, in an app or at a remote merchant site.

Contactless mobile wallets and digital wallets, i.e., Click to Pay[27] for online checkout (offered by the card networks), securely store payment tokens or actual payment credentials for merchants and other ecommerce businesses. Merchants do not collect and store customer payment credentials or PII on their websites or files, thus eliminating an attack vector for fraudsters.[28]

The *EMV Secure Remote Commerce* (SRC) Click to Pay remote checkout wallet specification promotes security and interoperability within the card payment experience in a remote payment environment. Its goal is to simplify and securely enable customers to pay online by protecting their payment information with a cloud-based wallet that stores customer PANs and related card/PII data in a secure system for each card network. Registered customers have a consistent one-click checkout when making a purchase on a website, mobile app or any other digital channel with an Amex, Discover, Mastercard or Visa credit, debit or prepaid card. This digital wallet

26 All NFC contactless mobile wallets accept any eligible branded credit or debit card (Visa, Mastercard, American Express, Discover) from participating FIs and PayPal. Examples include Apple Pay, Google Pay and Samsung Pay.

27 Secure Remote Commerce (SRC) replaces the individual card brand "digital checkout" wallets – Amex Express Checkout, Masterpass, Visa Checkout and Discover – with a consistent, simple user experience and strong payment security protections for all sites and cards. The SRC brand is now "Click to Pay." EMV® Secure Remote Commerce Frequently Asked Questions

28 Mobile wallet is a service accessed through a mobile device, which allows the wallet owner to securely access, manage and use a variety of services/applications, including POS and remote/digital payments, identification and non-payment applications. The service may reside on the mobile device or be remotely hosted on a secured server or a merchant website. European Payments Council. 2019 Payment Threats and Fraud Trends Report. December 9, 2019.

standardizes the transaction process across multiple remote/ecommerce checkout environments and customer devices, using a "virtual payment terminal" to replace individual card-branded digital checkout wallets.

Authentication for Enrollment in Contactless Mobile and Digital Wallets

Authentication for enrollment in a contactless wallet requires provisioning a payment token either to a mobile device or the cloud, depending on the contactless wallet solution provider. Tokenization[29] is optional for Click to Pay, and provisions the token in the cloud. Token provisioning replaces the credit or debit card number and expiration date with a numeric code of same length, called a payment token, and a token expiry date.

The contactless mobile wallet provider or the Click to Pay card network acts as the token requestor (TR). The TR verifies customer-supplied registration data against internal data (email, billing address), checks the card verification value (CVV) and performs optional proprietary fraud tests. It also reviews other data elements (including age of the iTunes account if Apple Pay), device ID, history of phone activity, phone model, geolocation, etc. to develop a risk score for the ID&V[30] process. ID&V determines if the customer is the legitimate owner of the account credentials linked to a wallet.

The Token Service Provider (TSP)[31] or card network receives the encrypted PAN and token request from the TR and initiates ID&V. The TSP uses its fraud monitoring systems, risk management tools and cardholder information stored in the network database to review card history, perform velocity checks[32] and review accounts. It authenticates each data element, including device ID, device fingerprint, geo-location and IP address. It also validates the card security code (CVV), reviews customer enrollment attributes and transaction history, and conducts proprietary fraud tests. The TSP then calculates a risk score and sends it to the issuing bank to approve provisioning the payment token to the wallet.

The issuing bank completes the ID&V process by comparing the TSP's risk score to the risk tolerance level of the applicant's portfolio and adds internal intelligence to arrive at a risk decision. The issuer either approves the card for token provisioning, rejects it, or invokes step-up authentication if the risk score falls into a predetermined range.

29 EMVCo payment tokenization replaces a PAN with a non-sensitive value (payment token) that represents a card number for the purpose of payment processing. Tokenization protects payment data using a combination of techniques, such as secure storage of sensitive data or and/cryptographic controls, ensuring that an unauthorized party cannot mathematically reverse the token value to the original PAN. Token domain controls protect the token against unauthorized use. USPF, June 2019. EMV Payment Tokenization Primer and Lessons Learned

30 ID&V ensures that the legitimate cardholder of the PAN issued by the FI is interacting with the TR during request of a mobile payment token. This involves verification of the previously established identity of the cardholder. EMVCo Payment Tokenization Specification Technical Framework 2.0, September 2017.

31 Token service provider (TSP) is authorized to provide payment tokens to registered token requestors (e.g., merchants, wallet providers). EMVCo (2017, Sept). EMV Payment Tokenisation Specification – Technical Framework

32 Velocity checks monitor selected data elements that occur in certain intervals multiple times by identifying fraud patterns that test out stolen credit cards (e.g., user ID, IP or email address, phone number, device ID, card number/payment method, billing or shipping address). This helps merchants review repeated patterns that happen within a short period of time, e.g., a significant increase of transactions from one month with anomalies, e.g., all being shipped to a commercial, not a personal address. Velocity Checks and Fraud Prevention

If the request is approved, the TSP creates and encrypts a device-specific static token, then stores it in its token vault, along with the associated PAN. The issuer generates a unique shared key associated with the static token used to create a dynamic cryptogram for each transaction. If the customer is enrolling with a contactless mobile device wallet (e.g., Apple, Google or Samsung Pay), the TSP sends the token and shared key to the TR to store in the customer's mobile phone.[33]

If the merchant using Click to Pay participates in the card network's token program, the TSP will generate and store a token when a customer enrolls an eligible card with Click to Pay. The token will not be stored in the customer's mobile wallet. During checkout, the TSP will send the token to the merchant to process with the transaction, securing the PAN and lowering potential fraud for the merchant.

Vulnerabilities

Weak ID&V authentication can compromise card enrollment services by provisioning stolen PAN credentials to a new contactless mobile wallet or Click to Pay

- If the issuing bank has a weak ID&V or step-up process – or poor enrollment controls – it creates an opportunity for fraudsters to use passwords that are weak or obtained from data breaches or compromised KBA to enroll stolen cards in the mobile or digital wallet.
- The fraudster downloads the wallet app in the victim's name by using fake or stolen PAN credentials and PII, then adds a stolen credit or debit card to the contactless wallet or Click to Pay to make purchases.

Weak authentication enables fraudster to take over an existing contactless mobile or Click to Pay *wallet*

- The fraudster convinces the call center to disable the biometrics and reset a passcode to open a stolen mobile phone, and circumvents the step-up authentication process, including KBA and OTP.
- With access to the mobile phone, the fraudster can open the existing contactless wallet, add his fingerprint, then use the cards in the wallet for future purchases or add other stolen cards.

33 Wallet providers vary in how they provision tokens to the mobile phone or the cloud. Google and Samsung store the token key in the cloud and download limited use tokens to the mobile phone wallets.

Weak step-up authentication allows the fraudster to intercept OTP needed to validate the cardholder to PAN during provisioning process

- The issuer sends an OTP via SMS or email to the cardholder for additional validation as the owner of the card.
- The fraudster can intercept step-up OTP communication on the phone or send a phishing email to the cardholder and convince them to send the OTP to the fraudster, who then responds from his mobile device, for example, through SIM swapping. On-phone OTP generation is more susceptible to fraud than server-based OTP because the mobile phone is typically more vulnerable to attack.

ENROLLMENT in PAYMENT SERVICE PROVIDER (PSP) or PROPRIETARY MERCHANT WALLET

This use case covers enrollment in online/mobile remote payment accounts initiated by mobile devices using a third party mobile app or browser wallet, or through a merchant browser that accepts a third-party wallet.[34] The proprietary merchant[35] use case includes businesses with an online presence that require customer enrollment to make purchases on their websites. Customers register via mobile app or directly on the merchant website.[36] PSPs and most e-merchants accept eligible credit and debit cards from the major brands (Visa, Mastercard, American Express, Discover), and some allow customers to add their bank accounts, prepaid and gift cards and/or PayPal for funding.

PSPs are cloud-based, and store customer PANs or network payment tokens in lieu of PANs on file (CoF). Cloud-based merchant wallets also store customer payment credentials (CoF) and have the option to replace PANs with tokens.[37] Many, but not all, e-merchants have a mobile app, and some e-merchants only operate via mobile app.

Authentication

PSPs may provide another layer of security (e.g., two-factor or multi-factor authentication). Amazon customers include additional data during enrollment that enables them to receive an OTP each time they access their accounts or make a transaction. PayPal's second-factor security key is automatic and does not require additional steps during enrollment. PayPal automatically sends an OTP via SMS for the customer to enter, in addition to their passwords, when they login and initiate a transaction.

34 Examples include PayPal and Amazon Pay. Amazon Pay enables consumers to use their Amazon payment credentials stored in Amazon Wallet to pay on other websites.

35 Retailers and other merchants (e.g., grocery, QSR/gas stations, transit, ride-sharing, hotels, entertainment/ticketing, order ahead) offer proprietary mobile/digital wallets.

36 Customers using guest checkout authenticate by providing PII and payment credentials each time they make a purchase.

37 Some merchants tokenize PANs for storage on the back end after the transaction has occurred, known as security/acquirer tokenization. Card networks are working with merchants to replace PANs on file with EMV payment tokens. These functions do not occur at enrollment.

PSPs and merchant/acquirers may perform extensive proprietary risk analysis, including fraud scoring, data analysis and back-end risk assessment; review of customer enrollment attributes or transaction history; verifying the e-mail and billing address; and collecting mobile device data (such as device fingerprint, device ID, IP checks, IP address and velocity).[38] If ID&V results in a high risk score, the FI may perform step-up authentication via KBA or send an OTP to the customer for verification.

Vulnerabilities

Fraudsters enroll by creating a new PSP or proprietary merchant account with a fake email address that they can use later with stolen credentials (username and password) to make a remote purchase.

TRANSACTION AUTHENTICATION ACROSS REMOTE WALLETS

This use case includes remote payment transactions initiated from a mobile/digital, PSP or proprietary merchant wallet transaction. It assumes that identity verification of the account owner occurred during enrollment in a wallet or PSP service, and therefore, the identity is approved to initiate transactions.[39]

Authentication

- *Contactless mobile wallet with stored credit or debit card:*
  The mobile app interacts with the native mobile wallet API to initiate payment with the card network and verifies the token. The cardholder authenticates with a biometric (e.g., fingerprint) or PIN on his or her mobile device. The issuer performs a risk assessment.

- *Click to Pay (EMV SRC) for digital checkout purchase by selecting linked debit or credit card:*
  To make a purchase, the customer clicks on the Click to Pay checkout button icon at the merchant website. SRC displays the payment cards stored with the customer's SRC Profile. The customer selects his or her payment card, confirms payment and shipping information, then completes the transaction. Once the checkout process completes, the requested data is returned to the merchant with the PAN or a payment token (if the merchant participates in the card network's token service) to submit to the payment service provider.

38 Behind the scenes, the PSP also may collect transaction and expense data, transaction dollar amount sent or paid, merchant data, funding instrument, device information, usage data and geolocation.

39 P2P transaction and enrollment authentication is covered in the P2P section.

- *PSP, proprietary merchant app, in-app or online merchant mobile/web browser login and purchase using linked bank account, credit or debit card:*
  The customer logs into a merchant app with username/password or biometrics, then selects the purchase. He or she enters the address (or verifies it, if prepopulated) and proceeds to checkout. The customer selects the payment method, which automatically appears if the customer preregistered.[40] If the customer selects PayPal, the system redirects them to the PayPal site for authentication.

  The merchant verifies account username and password in its own system, or the mobile device verifies biometric credentials if the mobile payment app has enabled biometric authentication.

  If funded with a credit or debit card, the card network performs additional risk management, and then transmits it to the issuing bank for authorization. If all parties participate in 3D Secure (3DS),[41] and depending on the transaction risk score received from the card network, the issuer may invoke 3DS/step-up authentication.

Vulnerabilities

- Fraudsters are extremely sophisticated. Through testing and limited attacks , they typically are able to identify which targets (i.e., merchants) are protected by certain fraud detection and prevention technologies, and which are not. Furthermore, fraudsters may work together, sharing collected intelligence to maximize the impact of their attacks. As part of this collaborative approach, fraudsters can disseminate information about detection gaps in real time and launch instant, massive and automated attacks to poorly protected or exposed targets.
- Identity thieves can defeat the basic framework for MFA – an OTP sent by SMS – if they can hijack a customer's phone number through porting or SIM swap.
- Customers often save credit card details in their store accounts, trusting merchants to guard them. Once fraudsters have accessed an account, they can lock out the owner by changing the security questions and passwords.

40 If funded with a bank account, customers can preregister the bank account with PayPal, Uber and some online retailers.

41 3-Domain Secure (3DS) 2.0 is a secure messaging protocol that applies risk-based authentication. It replaces passwords with complex authenticators, such as biometrics and OTPs, and enables issuers to authenticate cardholders in real time during an online or mobile-initiated transaction. Based on the transaction risk score, the issuer determines the risk level and decides whether to approve the transaction or challenge the customer by requesting another authentication factor to verify his or her identity. EMV® 3-D Secure

CONCLUSION

The objective of this brief is to describe types of payment authentication fraud and present examples of use cases to explain how customers authenticate when enrolling in an online banking or PSP/merchant website or making a financial transaction (paying for a remote purchase or transferring funds to another individual) with different payment methods, and where fraud may occur during the authentication process. Brief #3 will cover fraud mitigation approaches, present key findings and provide recommendations.

Mention or display of a trademark, proprietary product or firm in this report does not constitute an endorsement or criticism by the Federal Reserve System and does not imply approval to the exclusion of other suitable products or firms.

For more information, visit FedPaymentsImprovement.org and submit or update your FedPayments Improvement Community profile and select "Remote Payments Fraud" as a topic of interest.

THE **FEDERAL RESERVE**
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.