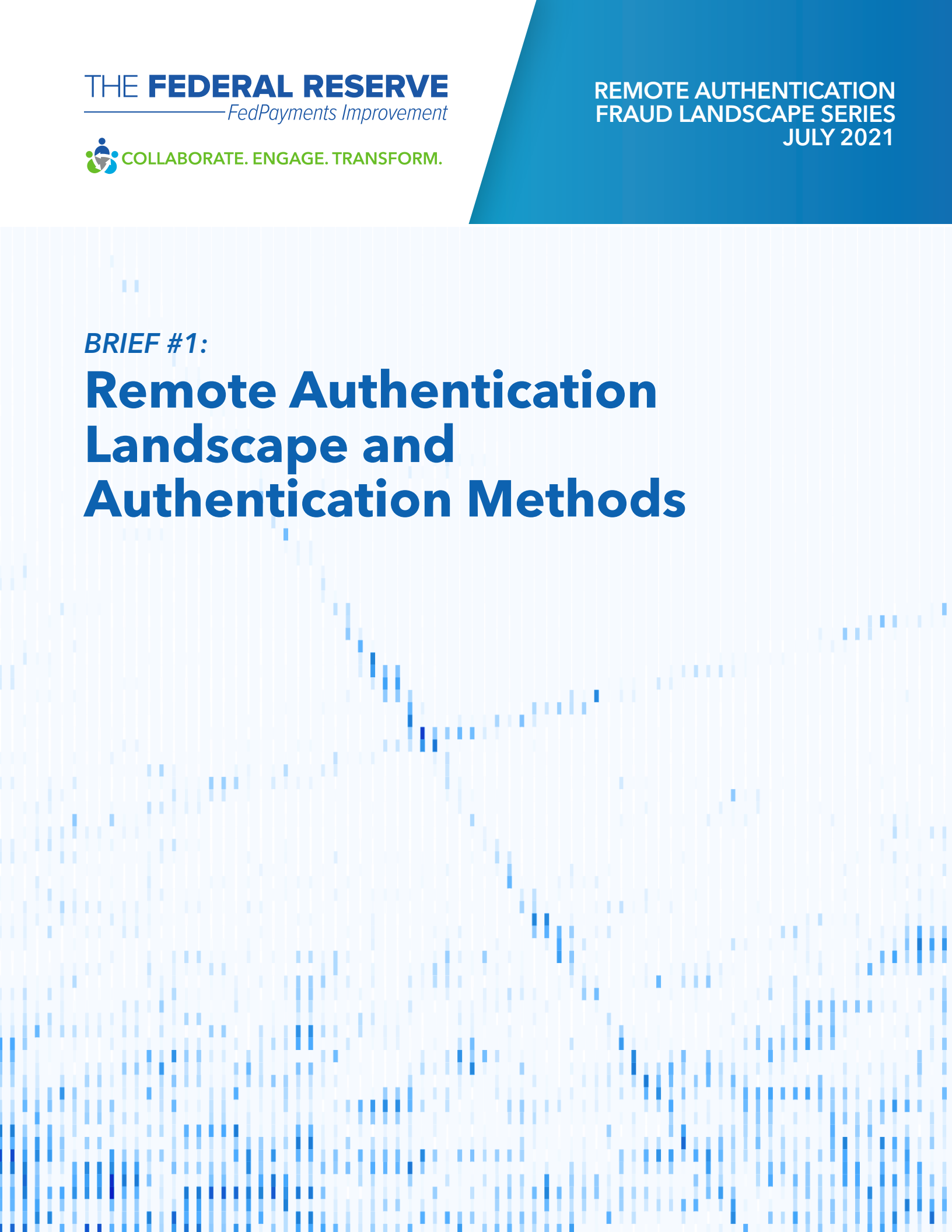
THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

REMOTE AUTHENTICATION
FRAUD LANDSCAPE SERIES
JULY 2021

BRIEF #1:

Remote Authentication Landscape and Authentication Methods



OVERVIEW

Brief #1 is the first of three research briefs in our series on the remote authentication fraud landscape. It describes types of authentication fraud and authentication methods used to prevent fraud. Brief #2 describes how stakeholders apply authentication in several remote payment use cases during the enrollment and the transaction process, and brief #3 discusses approaches and tools used in the payments industry to mitigate remote authentication fraud, key findings and recommendations on next steps to build awareness and engage industry stakeholders. Together, the three briefs cover the remote authentication landscape in the United States, including challenges and opportunities to reduce authentication fraud.

Methodology

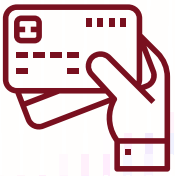
A combination of publicly available industry research and interviews with several payments and fraud experts were utilized to gather information on key challenges and mitigation efforts related to third-party (versus first-party) remote authentication fraud in the United States. The information was then used to develop this series of briefs. The objective is to describe the risks, challenges and mitigation to build awareness and educate industry stakeholders dealing with increasing payments fraud, particularly when fraud occurs during authentication.

Description of Remote Authentication Fraud

This brief defines remote authentication fraud 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. It can occur when the legitimate owner conducts a digital financial activity, i.e., via a mobile phone app, mobile browser or personal computer (PC) internet browser to: (1) open a bank account or credit card through mobile or online banking, (2) enroll a bank account or credit card with a third-party payment provider/digital wallet, (3) pay for a purchase or (4) transfer funds. In all cases, the customer is not present physically at the financial institution (FI) or merchant point of sale.

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/digital wallet



Pay for a purchase

Transfer funds

FIs struggle to control the mass availability of their customers' stolen personally identifiable information (PII), manage the rate of their new remote account openings, and keep abreast of new, sophisticated identity fraud schemes that enable remote authentication fraud. This problem has been exacerbated by increased accessibility to digital channels, which has led to growth in digital financial activity (e.g., account openings, transactions and non-monetary offerings).

The payments industry uses a myriad of authentication tools to prevent remote fraud attacks, but many financial institutions, payment service providers (PSPs)[1], processors and merchants rely on outdated authentication and verification methods to prevent payments fraud. Identity verification and authentication are not the same, but they are complementary. Verification confirms the identity of the customer by making sure the information provided about the person is accurate (e.g., official identity documents, date of birth, address, other PII). Verification usually is performed only when an account is created.

Authentication should occur during enrollment and each time a user attempts to access an account.

Authentication should occur during enrollment and each time a user attempts to access an account. Authentication confirms the activity is initiated by the verified user of the account through various factors, e.g., username and password, biometrics, to ensure the user is who he or she claims to be and is authorized to perform a transaction.

FIs that offer digital account opening employ a variety of safeguards, including some form of identity verification. It can be complicated to digitally verify the identity of a remote applicant and protect the account opening and transaction process against fraud. Effectiveness may vary depending on the authentication methods used. Not all digital payment service providers or merchants use advanced verification techniques to enroll new customers in their online payment services. This makes it easier for fraudsters with stolen PII or credentials[2] to use the customer's account for purchases or to transfer funds. Because fraudsters may have payment credentials previously gained from social engineering, strong authentication systems are needed to detect attempts to use the credentials to bypass fraud mitigation strategies and access customer accounts.

1 Payment service providers (PSPs) offer merchants the support they need to access electronic payments, including credit cards, digital wallets and bank accounts. PayPal and Stripe are examples of payment service providers. What is a Payment Service Provider or PSP?

2 Online banking or payment credentials are unique identifiers used by consumers when they are accessing systems that transmit financial data. These credentials may include username, password, a smart card with a built-in microprocessor, token or a biometric.

Heightening the need for greater attention to authentication fraud, COVID-19 is driving more consumers to enroll in online or mobile (digital) accounts to make remote payments. Industry survey data report that the average consumer e-commerce spending has increased significantly since the pandemic began in Europe. In the U.S., the average online consumer spend was 36% in December 2020, up from 26% in March 2020.[3]

Payments stakeholders[4] need to do more to stay ahead of fraudsters, who continue to look for new ways to execute fraud schemes by taking advantage of remote payments channel vulnerabilities to ascertain the identity of a consumer during onboarding, enrollment, login and transaction processes. In June 2020, the Office of the Comptroller of the Currency (OCC) published its Semi-annual Risk Perspective report that highlighted financial institutions' compliance risks during the coronavirus pandemic. The authors indicated an increase in the risk of fraud and potential for exposure of customers' sensitive information, as well as the expectation that malicious actors would continue to target the financial industry with disruptive attacks through phishing, destructive malware, ransomware and other cyberthreats.[5]

Fraud in Context

The seesaw analogy (see Figure 1) depicts the relationship between fraud activity and fraud prevention to illustrate how fraud fluctuates up and down over time. At some points in time, fraud attacks are more successful than efforts to stop them. In response, FIs and other payments stakeholders may implement or expand their fraud controls and mitigation efforts to limit the impact of fraud attempts. One example was the U.S. migration to EMV chip cards several years ago, which reduced counterfeit card fraud. However, many fraudsters then shifted to remote card-not-present (CNP) fraud. This led EMVCo to enhance its 3D-Secure (3DS)[6] protocol to incorporate risk-based authentication to address increased CNP fraud. As a result, fraudsters shifted to compromising the identity of an account holder at every step of the transaction lifecycle to conduct payments fraud.

While it is key to have strong authentication at every step in the process, it is especially important to implement authentication controls as far upstream as possible (i.e., at account opening and login). If organizations can stop the fraud before the transaction occurs, their loss risk will be dramatically lower.

3 Deutsche Bank Research/The Future of Payments: Series 2. Part 1. Post Covid-19: What Executives are Thinking and Doing. January 2021.

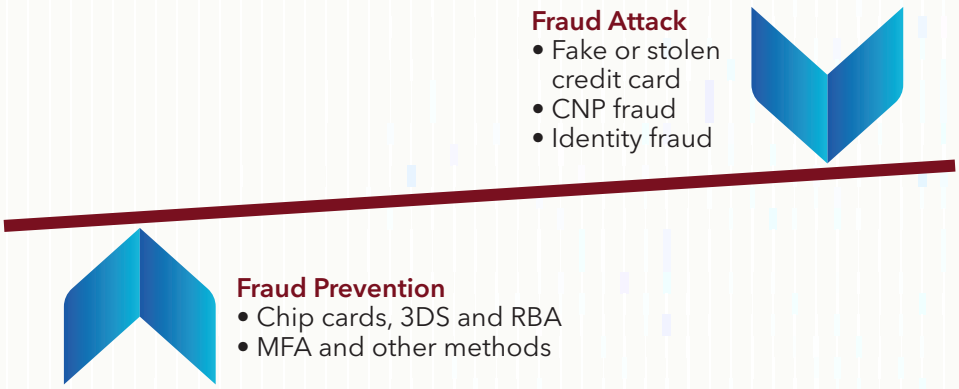
4 Payments stakeholders include financial institutions, core payment processors, payment service providers (PSPs), payment networks, merchants and other solution providers that sell goods and services online or remotely.

5 The OCC noted that banks' risk management programs should maintain effective controls for third-party due diligence and monitoring and other oversight processes, operational errors, heightened cybersecurity risks and potential fraud related to stimulus programs. Semiannual Risk Perspective, Spring 2020

6 EMV 3-D Secure (EMV 3DS) is a messaging protocol that provides global interoperability and a consistent consumer experience. It supports app-based authentication and integration with digital wallets, as well as traditional browser-based e-commerce transactions. The protocol permits the issuer to use risk-based authentication (RBA) in the background to prompt step-up authentication (e.g., OTP, biometrics and out-of-band) for higher-risk transactions, significantly reducing consumer friction and replacing static data (e.g., passwords, pre-established question responses, card expiration dates). EMV 3-D Secure protocol and core functions specification. Available at https://www.emvco.com/emv-technologies/3d-secure/

Establishing the right balance between fraud controls and a convenient customer experience can be challenging. FIs must secure customer payments, while ensuring authentication measures do not inconvenience consumers to the extent that they abandon the onboarding process or transaction before completion. Authenticating users at key steps in the payment process as the transaction moves from merchant to payment network to bank/issuer can help to prevent fraud and deliver an accurate assessment of risk.

Figure 1: Dynamic relationship between fraud activity and fraud prevention



The digital nature of the payment system has significantly changed the way customers can conduct banking and payment functions remotely via mobile and digital channels. They can quickly and conveniently open new bank Demand Deposit (DDA) and credit card accounts, create third-party and merchant accounts, pay for e-commerce purchases and transfer funds in real- or near real-time, from any location. However, these added conveniences increase opportunities for new account fraud, synthetic identity fraud and account takeover.

- *New account fraud (NAF)*, generally defined as fraud that occurs on an account within the first 90 days, where the account holder opened the account for the sole purpose of committing fraud. The process of establishing a new bank or credit card account may be done in person at a branch, or by accessing the financial institution's website via browser or mobile app.[7]

- *Synthetic identity fraud (SIF)* is the use of a combination of PII to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.[8]

- *Account takeover (ATO)* fraud is defined as obtaining a legitimate user's details to take over his or her online accounts, possibly enabling monetary or credit card theft. ATO can happen with an automated script that enters credentials all at once or with a human typing them and accessing the account. The goal of ATO is to make a profit using the value of the account.[9]

7 New account fraud verification procedures vary among financial institutions but have become more standardized since the USA PATRIOT Act passed in the wake of the terrorist attacks of September 11. A primary provision of the act mandates FIs to establish policies and procedures to reasonably verify the identity of all parties seeking to open an account. Financial Institution Fraud

8 In 2018, the Federal Reserve launched an initiative to raise awareness and encourage action on the growing problem of synthetic identity payments fraud in the U.S. through primary and secondary research and industry dialogue. Outputs include three white papers and an industry-recommended definition. The Real Problem of a Fake Identity

9 What is an Account Takeover attack? Account Takeover Fraud Detection

AUTHENTICATION METHODS

Overview

This section describes several methods to authenticate an individual during remote enrollment and transaction processes, as well as types of data collected to verify the identity. Stakeholders need to have a good understanding of available authentication approaches and tools, including which are most effective depending on the payment type, customer information, transaction type and risk level.

Multiple authentication methods exist to confirm that the identity of an individual accessing and interacting with an account is the same individual whose identity was verified at enrollment.

Prior to authentication, identity (ID) proofing verifies an individual's connection to his or her real-world identity to assure the individual is who he or she claims to be.[10] Identity proofing occurs when an individual opens a bank or credit card account, signs up for a new banking service or adds a biometric method to the account for future authentication. Once a customer has a proven identity, the veracity of information provided to confirm the user ID is accepted.[11] Verifying identity and providing strong authentication are key steps to preventing the occurrence of fraud from the very beginning of the customer account relationship.

Authentication covers multiple steps, including enrollment with PSPs and online merchants, funds transfers and account recovery. Authentication can be explicit (e.g., requiring the individual to enter a passcode or perform a biometric check) or implicit (analyzing context, transaction, and device information to detect unusual behavior that could indicate fraud).

More specifically, authentication:

- Corroborates a claimed identity
- Validates that an entity is a real person, not a machine or bot[12]
- Affirms that an individual is not likely a fraudster
- Authorizes a specific financial request

10 The National Institute of Standards and Technology's (NIST) Special Publication 800-63-3, Digital Identity Guidelines calls for collecting and assessing multiple pieces of user-asserted evidence to make an identity-proofing decision and address ongoing PII compromises. www.nist.gov

11 Identity data may be verified against government sources. After vetting, the FI goes through authentication protocols, such as multi-factor authentication (MFA), to obtain consumer data and check it against proprietary data assets and outside credit bureau databases, e.g., Equifax.

12 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.

Description of current authentication methods

While there are many authentication methods to prevent remote fraud, these methods provide different levels of protection and may function independently of each other. Because of the changing nature of fraud, the effectiveness of some methods is declining. These methods are being replaced with stronger, but not widely adopted, alternatives across the payments industry. The sophisticated attacks to the payment system expose flaws in current authentication practices and create a need to develop more complex defense strategies. Multi-layered and multi-factor authentication (MFA)[13] are considered best practices for stronger authentication in the industry. If applied appropriately as a first step, these methods can help prevent authentication fraud from occurring later in the payment process.

Multi-layered authentication

Multi-layered approaches combine several authentication methods to confirm the identity of the account holder during onboarding, enrollment and when conducting a payment transaction. Layers can include passive[14] authentication data (e.g., mobile device intelligence, device binding, one-time passcodes or OTPs, license scanning), as well as username and password, knowledge-based authentication (KBA), biometrics, machine learning and behavioral analytics. While not prescriptive on which options to use, layering implies implementing at least two authentication methods, known as the waterfall process for identity proofing.[15] Layering enables the provider to use the appropriate authentication methods based on transaction value, type of mobile device and type of payment (new or recurring).

Multi-factor authentication requires use of one authentication method from each of three distinct factors: something you know, something you have and something you are.

13 Multi-factor authentication (MFA) helps to determine that users are who they say they are. The more factors used to determine a person's identity, the greater the reliability of the authentication. MFA combines the following factors:

- Something you know: password or personal identification number (PIN)
- Something you have: token or smart card (two-factor authentication)
- Something you are: biometrics, e.g., fingerprints (three-factor authentication)

14 Passive authentication does not require user action to obtain data.

15 Waterfall process involves multiple steps that must be passed to open an account, although the user can skip out of any step. The process generates a risk score at the end.

Multi-factor (MFA) authentication

Applying MFA to confirm the customer's identity when he or she logs into a remote banking or payment app makes it more difficult for an unauthorized person to locate the device, network or database and access the remote app. MFA takes layering a step further by requiring use of one authentication method from each of three distinct factors: something you know, something you have and something you are. Individually, any one method or factor may not provide enough protection from fraudsters. However, if one factor is compromised by a fraudster, having a second factor adds more protection to prevent fraudsters from obtaining enough information to authenticate and access an account. For example, if a fraudster enters a legitimate password, he also will need the registered device and biometric to make a fraudulent remote transaction. See Figure 2.

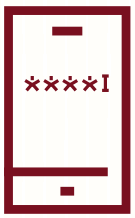
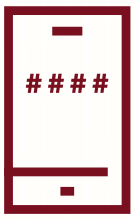
Figure 2: Description of Current Authentication Methods

SOMETHING YOU KNOW

Authentication Method	Authentication Description
Username and Password 	A username uniquely identifies the user. The password is a secret string of characters to authenticate the user as part of the login process on a device, within an app or online via a banking or payments site. Each provider establishes its own standards and requirements for how to create the username and password. FI passwords typically vary from eight to 12 characters and include one or more upper- and lower-case letters, digits and special characters. The password is static, but depending on a provider's rules, users may be required to periodically change their passwords or reset a forgotten password.
Personal Identification Number (PIN) 	A PIN is a static numerical code. Use of PINs has traditionally been associated with face-to-face point-of-sale (POS) and ATM transactions. Use of PIN is very limited for remote or CNP debit transactions, although some mobile network operators (MNOs) require PINs. PINs for credit card transactions, whether POS or remote, are virtually non-existent in the U.S.

Figure 2: Description of Current Authentication Methods *(continued)*

SOMETHING YOU KNOW

Authentication Method	Authentication Description
Knowledge-based authentication (KBA) 	KBA is a type of challenge-response authentication. It requires the user to answer secret questions that are pre-established with users (static) or randomly generated by the provider (dynamic). These can vary from very basic (e.g., mother's maiden name or birthplace) to more challenging facts that are easily recalled by the user but cannot easily be found in a physical wallet or online (e.g., current mortgage amount, high school mascot, first car).
Out-of-band (OOB) authentication 	Out-of-band authentication is different from, and therefore is less likely to be subject to, the same attacks as the primary communication channel employed by the parties that initiate the given transaction.[16] A customer receives a call on his or her phone to confirm the transaction or receives a text message (SMS) with a code to proceed with the transaction.
One-time Passcode (OTP) software token 	OTP is a method used to meet the 2FA requirement for a separate communication channel. An OTP software token is a dynamic passcode or PIN generated by software. This random number or code has a finite expiration time and is typically transmitted via email or over SMS to the mobile phone for customer verification. The OTP is only valid for a single use and intended for the person with full control and access to the device receiving the OTP.
Push Notification 	Push notifications send a message directly to a secure application on the user's device, alerting him or her about an in-band or out-of-band authentication attempt. Users view authentication details to accept or decline transactions or login requests, typically via the press of a button. Push notifications authenticate the user by confirming the mobile device registered with the authentication system is in the user's possession.

16 Out-of-band Authentication (OOBA) is an authentication process that utilizes a communications channel that is separate from the primary communication channel of the entity trying to establish an authenticated connection with the end-user. It must be different from, and not subject to, the same attacks as the primary communications channel employed by the parties to initiate the given transaction. By using two different channels, authentication systems can guard against fraudulent users that may only have access to one of these channels. What is Out-of-Band Authentication (OOBA)?

Figure 2: Description of Current Authentication Methods *(continued)*

SOMETHING YOU HAVE

Authentication Method	Authentication Description
Device fingerprint 	A mobile device ID "fingerprint" is an additional (passive) authentication factor based on the device configuration and proprietary vendor algorithms. It confirms the mobile device is the same as the device used to enroll or make a previous legitimate transaction. Most commonly analyzed mobile device characteristics are installed plug-ins, software and time zone, but also may include carrier ID (SIM authentication), phone "no risk" score, device type (web, mobile, IOT), secure elements, "jailbroken" status and geolocation.[17] These mobile tools are transparent to the user, reliable risk indicators and useful for detection.
QR (Quick Response) Code 	QR code authentication uses a mobile device camera to scan a QR code in lieu of a password or PIN for login to consumer-initiated payment mobile apps with PSPs or merchants that accept QR codes. The QR code is a randomly generated number that maps to the real Payment Account Number (PAN). The PAN is stored in a proprietary cloud (PSP or merchant) and not on the mobile device. Apps using QR codes to authenticate may also use biometrics to open the app before displaying or scanning the QR code.

17 Geolocation uses location technologies such as GPS or IP addresses to identify and track the whereabouts of connected electronic devices. It is used extensively in the financial services industry to help prevent fraud and give customers information about nearby services. Geolocation January 2021

Figure 2: Description of Current Authentication Methods *(continued)*

SOMETHING YOU HAVE/KNOW

Authentication Method	Authentication Description
OTP hardware token/ security key 	A hard token is a physical device that generates dynamic security codes the customer uses to authenticate during a logon process. The hardware security token is typically a pocket-sized device with a small screen (such as a USB token, display card or key fob) that generates and displays a single-use, unique multi-digit numeric code with a finite expiration time.

SOMETHING YOU ARE

Authentication Method	Authentication Description
Physical Biometrics 	Physical biometrics measure and analyze unique physical attributes of an individual for identification. Examples include fingerprint, facial or voice recognition, iris scans. Fingerprints are currently the most common method for mobile-initiated payments and banking, but customer acceptance of facial recognition has begun to increase as well. Facial recognition requires the user to take a selfie with their mobile device to validate their identity during a transaction or login process. The function compares the selfie to data collected when the user first registered their device.[18] The application must be able to detect impersonation by a fraudster.

Federal Financial Institutions Examination Council (FFIEC)[19] guidance requires that FIs implement layered security, consistent with the risk for covered consumer transactions, and recommends offering MFA to business customers. However, it does not mandate or endorse specific security techniques, leaving the door open for selective or minimal deployment of MFA. FFIEC has encouraged non-bank payment stakeholders to see the value of multi-layers and MFA in reducing payment authentication fraud.

18 65% of consumers are happy to provide biometrics to their bank; while 60% are open to using fingerprint scans to secure their accounts. FICO Survey Reveals U.S. Consumers Need to Better Protect Themselves When Banking Online

19 Federal Financial Institutions Examination Council (FFIEC) "Supplement to Authentication in an Internet Banking Environment." FFIEC Releases New Authentication Guidance for Online Banking. The guidance suggested bank security for online transactions was inadequate and that multi-factor, or equivalent, authentication techniques were necessary.

MFA Benefits

- Provides a higher level of security than single-factor or two-factor authentication.
- Provides some consistency with authentication approaches.

MFA Challenges

- MFA can increase customer friction when indiscriminately applied to all use cases and circumstances. If there are too many authenticators or they are too complicated, customers will abandon their online shopping carts. As a result, customers may choose easier, albeit riskier, MFA options (such as PIN or password) over stronger options, such as biometrics.
- Consumers are accustomed to using passwords, which are likely to remain the default first MFA factor for the near future. Forrester reports that 70% of organizations still rely on password-centric authentication.[20]
- While more providers are implementing MFA, anecdotal evidence suggests its use is inconsistent:
    - Lack of standardization and minimal data to measure the effectiveness of MFA complicate how to determine which vendor solution is most effective for a particular use case. As a result, many organizations are taking a "wait-and-see" approach or have implemented MFA only for their highest-risk portfolios.
    - The rate of change at which fraudsters are able to invent new fraud attacks has made some organizations wary of making incremental improvements. They may defer upgrades until the "next best system" has been identified.
- FFIEC guidance on multi-layered authentication focuses on FIs, although it encourages non-banks to consider MFA's value. However, it remains a gap that may put the broader payment system and consumers at risk, since payment instructions flow between, and therefore impact, FIs, processors, networks and merchants if all parties in the process do not apply effective authentication controls.

20 Passwords Belong in Time Capsules, Not IT Ecosystems, March 5, 2020.

Data collected to support authentication

The authentication methods described in Figure 2 work by collecting and analyzing multiple data points, which is why the ability to collect useful and verifiable data is key.

Data collection refers to the process of gathering data about the individual enrolling in a payment service or initiating a financial (banking or payment) transaction, the device used to conduct the transaction, and the type of transaction. Data collected for verification or authentication purposes comprise the attributes (identity, device, or knowledge) that describe an individual. Examples include name, email, fingerprint, swipe angle, apps loaded and internet protocol (IP) address. Some data is mandatory, while collecting other data may depend on the need or type of transaction, or as a best practice.

Organizations collect data elements from a variety of sources, initially when account ownership is established. The data strengthen over time through the above-mentioned techniques to provide a high degree of trust at account login and during a transaction.

Mandatory data

Financial institutions are required under Know Your Customer (KYC) and Customer Identification Program (CIP) regulations to collect, verify, and record a minimum set of data elements that provide evidence of a customer's identity at account opening or onboarding. Required data elements include name, date of birth, address, identification number (e.g., Social Security number) and documented evidence of identity and address.

Typically required data

FIs also collect digital and mobile identifiers, such as email address, phone number, preferred or registered device.

User-generated authentication data

Once the FI approves an application, the user is required to establish a username and password to access the account and then, to set up multiple security questions and answers, which account holders later use to re-verify account ownership or reset passwords.

Optional data

Advanced account opening processes that extend beyond standard KYC may ask for additional information to further identify and subsequently, authenticate the customer. Examples of optional data include PINs and biometrics (facial, fingerprint and voice recognition, selfies and video). For remote account openings, organizations may request biometrics to establish a link between the ID document holder and the ID document, or to establish that the applicant is a live person and not a bot – automated software that runs per instructions without human intervention.[21] Common techniques include CAPTCHA (distorted letters and numbers), and reCAPTCHA (i.e., a grid containing multiple photos where the customer selects grid boxes displaying a particular object).

Invisible authentication data

Organizations also can collect data about the behavior of the legitimate owner and his or her device through behavioral biometrics, behavioral analytics, advanced algorithms and device identification.

These techniques:

- Predict which transactions are normal or anomalous (e.g., type, size, frequency, location)
- Analyze biometric behavior typical to the account holder (e.g., typing speed, swipe direction, angle of handheld device) to detect automated bot or imposter attacks
- Examine all aspects of a device (operating system, IP address, geolocation, browser history and jailbreak status) to establish genuine ownership.

Machine-generated authentication data

When organizations detect an elevated level of risk or one that exceeds a certain threshold during login or when initiating a transaction, they communicate with the account holder to verify his or her identity. This is typically done by sending a code via SMS or email to the account holder's device, which the customer then keys into a field on the mobile or website.

21 When enrolling in a mobile banking app, mobile wallet, or mobile person-to-person (P2P) app, customers may have the option to activate their device-enrolled biometrics.

CONCLUSION

This brief provides an overview of how authentication occurs in the remote space, defines the primary types of authentication fraud, and explains different authentication methods and how they support multi-factor authentication. Brief #2 will provide more detail about account takeovers, new account fraud and other vulnerabilities. We also will describe how authentication methods are used to prevent fraud for several remote payment use cases during the enrollment and transaction processes.

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.