Fraud and Emerging Tech:

Identity and Authentication with the Paycheck Protection Program

July 2023

AFC

Since early 2020, many organizations have dealt with the consequences of the COVID-19 pandemic. One significant impact was the shutdown of the economy that caused organizations to close or limit their operations. The US government, tasked with providing economic relief to organizations and their workers, devised the Paycheck Protection Program (PPP), which helped organizations continue to pay their workers during the pandemic. During the program, more than $800 billion was dispensed with few requirements to ensure that the recipients were entitled to those funds. Proper controls could have mitigated the frauds that have since been uncovered, as many of them were the result of identity theft and falsification of documents.

Key control objectives are relevant to the prevention of PPP fraud. Much of the frauds that targeted the PPP were associated with falsification of identities and material information by fraudsters when applying for PPP loans through the various financial institutions (FIs) that were delegated authority by the Small Business Association (SBA) to process loans.

This article, part of an emerging technology series from the Anti-Fraud Collaboration, examines two key control objectives relevant to the prevention of PPP fraud and the technologies and processes concentrated on identity and authentication to mitigate identity-related frauds. This article also covers some of the technologies and processes that could have improved the verification of applicants' identities and could have reduced the number of frauds that occurred during the PPP.

The Need for Controls

The PPP first began as a $349 billion package of the Coronavirus Aid, Relief, and Economic Security (CARES) Act passed in March 2020. The PPP was increased to more than $800 billion, and the initiative was led by the SBA to help eligible organizations withstand the disruptions caused by the pandemic. PPP distributions were designed as "forgivable" loans, meaning that an applicant had to work with an authorized FI to complete an application and to provide supporting documentation to receive a loan.

The PPP largely met the objective of distributing money to millions of businesses quickly enough to brace the economy against the ravages of the pandemic. However, the PPP has been criticized for reports of widespread identity and eligibility fraud, largely enabled by stolen or forged documentation. From the onset of the PPP, fraudsters were able to use stolen or forged identities to obtain loans. Estimates of the total amount of fraud in PPP loans are reported to be more than $80 billion. The SBA Office of the Inspector General characterized the PPP's design of fraud mitigation controls as a "pay and chase" model, where fraud prevention relied mainly on the deterrent effect from the threat of prosecution. A strong control environment is essential as fraud related to PPP may occur from origination to forgiveness and repayment of the loans.

CONTROL OBJECTIVES

Organizations have an important responsibility to identify and authenticate any party they conduct business with such as a customer, a vendor, or any other stakeholder. Identity and authentication verification controls are critical to mitigating overall fraud risks, and those that take advantage of available technology can prevent many frauds. These controls can be used to confirm the identification of a party, affirm the protection of assets, and ensure compliance with program rules. Identification and authentication processes designed to establish a financial relationship with an authorized representative of a potential business customer are also essential to minimizing fraud risks.

Identity and authentication verification controls are critical to mitigating overall fraud risks, and those that take advantage of available technology can prevent many frauds.

Although many reported cases of PPP frauds focus on unapproved uses of the funds—which can be discovered only after the fact in a review of loan forgiveness documentation—illegitimate applications based on stolen or forged identities or documents were all fraudulent. Improving controls to prevent identity theft and misrepresentation would have mitigated a substantial portion of the program's risks. To prevent the PPP's frauds that started with identity theft, two key control objectives can be summarized as:

+ **Identity:** What were the applicable small business entities, often called the target population, for whom the program was intended? Which persons were authorized to apply for a loan on behalf of each entity?

+ **Authentication:** How did the FI verify whether the person claiming to be an authorized decision maker for an entity was who they said they were?

CONTROL GUIDANCE AND TECHNOLOGIES

For government programs like the PPP, enterprises and some organizations may be required or motivated to screen authorized

representatives of potential business customers. Identity verification controls are critical to mitigating financial fraud risks. Organizations can leverage identity verification controls to verify and screen customers or third parties who have a history of fraud or misconduct.

Digital identity control guidance for government information systems, including those run by the SBA, is published by the National Institute of Standards and Technology (NIST), primarily in the Special Publication (SP) 800-63 series on digital identities. NIST also publishes SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," which contains a broader technology control framework that includes best practices for relevant processes for organizations to implement, in areas such as account management, risk assessment, risk management, access control, and monitoring. Organizations can leverage this framework to strengthen their authentication and identification controls to prevent fraud.

Other US government agencies, such as the Department of Homeland Security, Internal Revenue Service (IRS), Social Security Administration, and Federal Bureau of Investigation, provide identity verification services under various conditions, including the use of biometric data to reduce the likelihood of impersonation. The agencies work with each other and the private sector to promote anti-fraud efforts, including making identity verification services available via application programming interface (API) connections to government databases. Organizations can use the processes and services from these agencies to strengthen their anti-fraud procedures and controls.

Identity

A fundamental control for a technology-enabled system is the definition of relevant identities (IDs) to which differentiated roles and permissions may be assigned. Associating actions with vetted and verified IDs enables accountability through the enforcement of preventive, detective, and remedial controls. NIST describes digital identity controls as mainly consisting of "proofing" and "authentication."

The PPP can be viewed as a federal information system that directly involved the SBA, FIs, and applicants who represented demonstrably eligible entities. For the PPP, the SBA relied on and expanded access to its existing loan processing system, known as E-Tran. Although E-Tran had fraud prevention, detection, and monitoring capabilities, largely enabled by its API connections to government agencies' databases, the PPP suspended numerous controls and authorized FIs to approve their own applications. Controls that were suspended and not implemented by the SBA included reluctance to conduct formal fraud risk assessments, a lack of anti-fraud controls in the PPP loan origination process to lock bank account changes after the lender verification process, and disbursement of funds without running a credit check on applicants. The relaxing of these controls, along with others that were suspended and not implemented, contributed to PPP frauds. Any organization that suspends various controls related to financial reporting exposes itself to risks of financial fraud.

DIGITAL IDENTITY GUIDANCE

NIST SP 800-63-3, "Digital Identity Guidelines," defines identity proofing as the initial process of verifying the authenticity of an individual's identity credentials and associating them in a database record with a unique digital ID. Authentication is a subsequent verification that the user of a digital ID is its owner.

ELIGIBLE BUSINESS IDS AND AUTHORIZED INDIVIDUALS

The population of eligible recipients described in the CARES Act included small business concerns (as defined in the Small Business Act), plus other types of organizations, generally with fewer than 500 employees, such as sole proprietorships. The CARES Act also required each PPP loan to be registered using the borrower's TIN, which enabled additional controls and provided an audit trail to help ensure accountability. The borrower was the small business, which could represent an organization with up to 500 employees.

The CARES Act did not specify criteria for the owner of the bank account that received the funds on behalf of an eligible entity, though it did specify that no collateral or personal guarantees were required from the applicant. The SBA delegated the authority to make and approve PPP loans to the submitted FIs. The PPP's design relied on the FIs' loan applicant proofing procedures to verify the identities of the business entity borrower and the individual applicant, as well as the applicant's authority to take custody of the borrower's funds. The PPP's design also relied on the FI to approve its own customer due diligence (CDD) and identity verification error resolution efforts, which is not consistent with proper segregation of duties. Errors in the identity verification process can contribute to potential fraud risks in an organization.

ENTITY AND APPLICANT ID VERIFICATION

For an applicant to apply for a loan as part of the PPP, the borrower's Taxpayer Identification Number (TIN) could be either an individual's Social Security Number (SSN) or a business ID, officially known as an Employer ID Number (EIN), which is issued by the IRS. When the TIN is an SSN, the only authorized applicant is the owner of the SSN. However, when the TIN is an EIN, more than one person may be authorized to submit a loan application on behalf of the business, and the FI might even require more than one person to authorize the transaction in some cases. For example, some business accounts may require dual authorization, such as from the CEO and CFO. Organizations can consider implementing dual authorization controls when approving loans to strengthen their financial reporting controls.

The IRS uses the EIN to distinguish specific taxable entities, although the application form to obtain an EIN requires only that a single "Responsible Party" be submitted for the account. The IRS described this as the "person who ultimately owns or controls the entity or who exercises ultimate effective control over the entity" and elsewhere as the "principal officer." Unlike common commercial account management best practices, the EIN does not use role-based access controls to differentiate the permitted actions granted to beneficial owners and authorized management representatives, nor does it have a field to submit related EINs that could be used to identify affiliated entities. The absence of such information impedes the automation of verifying an individual's claim to be an authorized representative of an organization. The IRS's EIN database does not systematically capture and distinguish between the beneficial owners and authorized management representatives with sufficient additional data (e.g., SSN and account role) to feed an API that could enable an automated verification service.

BORROWER "SELF-CERTIFICATION"

The Pandemic Response Accountability Committee (PRAC) review of 66 PPP criminal cases prosecuted by the Department of Justice for loans made in 2020 found that PPP loan applicants misrepresented information in 100% of the cases, including 91% where forged or altered supporting documentation was submitted. The PRAC concluded that even after enhanced controls were put in place for PPP loans made in 2021, fraudulent applications including fake documents and borrower misrepresentations could be approved.

Some of the mandatory CDD controls for FIs cover identification and verification of the beneficial owners of legal entity customers, such as businesses. The CDD rules require that an FI record and verify, among other data, the beneficial owners' dates of birth and TINs. The SBA required PPP lenders to verify the identity of the borrower and the business by confirming the taxpayer identification number, legal name of the business, and business address. The SBA indicated to the PRAC that if PPP lenders applied know-your-customer requirements more consistently, more frauds would have been identified. As part of their anti-fraud efforts, organizations can apply in-depth CDD processes to verify vendors, third parties, employees, or other stakeholders they engage with who do not have past incidents of fraud or misconduct.

Authentication

As described by NIST, authentication is the process of verifying that the holder of a credential such as an SSN or EIN is the authorized user of the credential. Authentication factors are often described as consisting of:

- **Something you know,** such as a password, date of birth, or mother's maiden name. Not all types of this factor are equally secret or secure.
- **Something you have,** such as a cell phone or other device with an application synchronized with a real-time identity service.
- **Something you are** (or can perform), such as a thumbprint, signature, or voice pattern, which are often called biometrics.

When a process uses more than one type of authentication (often referred to as multifactor authentication), it improves the strength of the control by reducing the chance that an impostor would have or know multiple pieces of the required information.

When a process uses more than one type of authentication (often referred to as multifactor authentication), it improves the strength of the control by reducing the chance that an impostor would have or know multiple pieces of the required information.

LEVELS OF ASSURANCE

The NIST SP 800-63 guidelines identify three identity assurance levels (IALs):

- IAL1: No requirement or process is needed to link the applicant to a specific real-life identity. The process may accept zero or more self-asserted attributes from the applicant.
- IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. Proofing can be done remotely or in person.
- IAL3: Physical presence is required for identity proofing, and identifying attributes must be verified.

The NIST guidelines further describe categories of identity evidence and verification, with biometric data included in strong and superior types. Remote verification of biometric data can be done with superior quality, if certain requirements are met, such as high-resolution video transmission, live participation by all parties, or properly trained reviewers.

Traditionally, applying for a business loan has been treated as an IAL2 or IAL3 transaction. Recently, advances in technology have increased the use and reliability of remote methods for proofing new customers. For example, businesses can subscribe to web-based services to verify certain passport and driver's license data. Additionally, advances in mobile communication technology have enabled ubiquitous video conferencing, which further diminishes the distinction between the quality of physically present and remote interactions.

IAL2 and IAL3 methods require the collection, validation, and verification of specified types of information from authoritative sources. The guidelines also identify steps that must be taken at each level for the control to be effective. The PPP loan process was designed to collect information like an IAL2 or IAL3 process; however, by instructing the FIs to rely on borrower self-certifications, the process was effectively downgraded to IAL1.

Although the CARES Act did not specify rules for determining who was authorized to apply for a PPP loan on an EIN's behalf, the SBA's "[PPP] Loans Frequently Asked Questions (FAQ)" document clarified that lenders could rely on the signature of a single borrower as sufficient representation of their position as an authorized representative of the small business. Although a signature can be used as a biometric factor of authentication if its performance is physically observed and compared against a previously registered version, the PPP loan application process merely used it as an acknowledgment of both the terms of the loan and the consequences for misrepresentation.

Over the course of the PPP, there were instances where FIs did not apply proper know-your-customer controls, which permitted frauds to be perpetrated. The risks of relying on IAL1 controls for financial transactions are well known. While relying on IAL2 or IAL3 controls, organizations can minimize financial fraud by implementing multifactor authentication processes with financial transactions to ensure that the intended parties are authenticated, and the transactions are safeguarded.

BIOMETRIC AUTHENTICATION

For IAL3 transactions, the NIST guidelines state that biometric data must be collected and recorded at the time of proofing, either in person or supervised in real time remotely, to satisfy the objective of nonrepudiation. For IAL2 transactions, biometric data are optional, but if used properly, biometric data can reduce the number of pieces of evidence necessary to provide strong controls. According to the NIST SP 800-63 guidelines, one way to enhance the quality of some biometric authentication controls is to train individuals to properly perform manual reviews of the match between a credential user's biometric characteristics and the official record, which may require some judgment. Organizations can consider implementing biometric authentication as part of their anti-fraud controls related to financial reporting and transacting and can train their employees on performing reviews of biometric data to detect fraudulent biometric authenticators.

BIOMETRIC AUTHENTICATORS

Some widely used biometric authenticators include:

+ Signatures
+ Photographs (face recognition)
+ Fingerprints
+ Palm prints
+ Iris scans
+ Voice pattern
+ Dental records
+ DNA

Conclusion

The PPP's failures were largely a result of inadequate fraud prevention controls, particularly regarding identity verification and authentication. The PPP could have taken advantage of available technologies to automate and enforce controls over identity and authentication; however, the SBA instead adopted and publicly communicated a "pay and chase" approach that almost certainly signaled an opportunity to commit fraud to those persons inclined to such endeavors. Identity verification controls that use sound CDD processes and biometric authenticators should incorporate diverse methods to mitigate fraud risks. Organizations can collaborate with regulators to share identity verification information and to strengthen controls where possible, including using biometric authentication, to make it harder for people to commit such frauds in the future.

Where can I learn more about identity and authentication?

- BDO: *5 Steps for Adopting a Zero Trust Model*
- BDO: *Three Top Cloud Security Challenges Facing Companies*
- Crowe: *A Guide to Using Analytics to Control PPP Loan Risks*
- Crowe: *Why Multifactor Authentication Matters*
- Deloitte: *The Future of Digital Identity: What Does It Mean to You?*
- Deloitte: *Trends in Digital Identity with Mike Wyatt*
- EY: *Digital Identity Now: From Security Control to Organizational Enabler*
- EY: *The Great Convergence: Portable Digital Identity*
- FEI : *Fraud in 2022: How Finance Leaders Can Fight Back*
- FEI: *How to Defend Against Social Engineering Attacks in Banking*
- Grant Thornton: *Apply Zero Trust Without All the Pitfalls*
- Grant Thornton: *Tips to Strengthen Your Company's Passwords (And Yes, They Need Strengthening)*
- IIA : *Auditing Identity and Access Management*
- IIA: *On the Frontlines: Auditing Human Factors Risk*
- KPMG: *Finding Your Blind Spot: Authentication Strategies to Reduce Identity Fraud*
- KPMG: *The Future of Authentication Is Here*
- KPMG: *The Future of Identity & Access Management*
- NACD : *Eight Questions to Frame Data Privacy Discussions in the Boardroom*
- NACD: *The Top Risks for the Next Decade: A Global Perspective*
- PwC: *Does Your Customer Identity and Access Management (CIAM) Inspire Trust?*
- PwC: *Manage and Secure Third-Party Risks with Identity and Access Management*
- RSM: *Detecting and Preventing Fraud for PPP Loans*
- RSM: *The Top Trends in Identity Management*

AFC

www.antifraudcollaboration.org

We welcome your feedback!

Questions or comments?
Visit antifraudcollaboration.org/contact