Federal Reserve
Bank *of* Atlanta

NO. 1—2025 October 2025
Payments Forum Publication

Using Digital Identity to Support Access to Payments

Kenneth Myers, Federal Reserve Board of Governors
Megan Rodden, Federal Reserve Bank of Chicago
Lali Shaffer, Federal Reserve Bank of Atlanta

The Federal Reserve Bank of Atlanta plays several key roles in the payments industry, including operator, supervisor, and researcher in support of the System's mandate of stable prices and maximum employment. Payments accessibility falls within the Federal Reserve's role to promote safety and efficiency in our nation's payments systems. Find more research and sign up for email updates at atlantafed.org/forms/subscribe.

Abstract
The rapid growth of digital payments, driven by technological advancements and a digitally dependent economy, has significantly enhanced financial access for consumers and businesses. However, some consumer segments may be distrustful initially of the technology and face barriers relating to stringent identity verification requirements. This paper explores possible digital identity technology solutions to support financial access amidst the expansion of digital payments and financial services while aiming to prevent fraud and ensure regulatory adherence.

The analysis, conducted by the Federal Reserve Bank of Atlanta and others, examines these barriers and gathers subject matter experts to identify how to incorporate solutions for enhanced compliance, risk management, and financial crimes prevention. The study highlights that current technology, when implemented safely, can effectively carry out identification and authentication processes, offering benefits such as cost efficiency, administrative efficiency, enhanced privacy, and fraud protection.

Key findings
- Adopting new technologies can improve efficiency in processes like know-your-customer and onboarding new accounts, provided they are implemented properly.
- Beneficial use cases include opening accounts remotely, sending cross-border remittances, and verifying public benefits.
- Digital IDs could streamline compliance processes, reduce costs, and enhance privacy and security.
- Challenges to adoption such as digital divides, authentication barriers, and public concerns still remain.
- Despite concerns, digital identity solutions could increase reliance by safeguarding data with enhanced technology.

JEL classifications: O32, O33, E42, D12

Key words: payments access, payments inclusion, financial inclusion, digital identity, consumer identity

https://doi.org/10.29338/pa2025-01

About the authors
Lali Shaffer is a director in the Payments Forum at the Federal Reserve Bank of Atlanta.
Megan Rodden is a senior payments policy analyst for Payments System Improvement in Federal Reserve Financial Services at the Federal Reserve Bank of Chicago.
Kenneth Myers is a principal IT architect in Information Security at the Federal Reserve Board of Governors.

Acknowledgements
The authors thank Jessica Miller, Krista Tedder, and our subcommittee of subject matter experts for their comments and assistance. The views expressed here are the authors' and not necessarily those of the Federal Reserve Bank of Atlanta or the Federal Reserve System. Any remaining errors are the authors' responsibility.

Comments to the corresponding authors are welcome at lali.shaffer@atl.frb.org.

SECTION 1 – INTRODUCTION AND BACKGROUND

The strong growth of digital payments, further accelerated by enhanced technology, has led to questions about how to ensure financial access to an unbanked or underbanked population in an increasingly digitally dependent economy. However, many consumers face barriers stemming from customer identity verification requirements, which are critical from a supervisory, compliance, risk, and financial crime standpoint.[1] Digital identity (ID), or the unique representation of a subject engaged in an online transaction,[2] could help facilitate the adoption of practices and guidance needed to protect consumers and businesses by improving the efficiency of identity verification, reducing financial crime, and promoting access to financial services.

The purpose of this paper is to explore digital identity technology solutions to support financial access alongside the growth of digital payments and financial services. At the same time, it is also important to understand the impact this innovation could have toward combatting money laundering and terrorist financing. In 2021, the global standards body for anti-money laundering and countering the financing of terrorism, the Financial Action Task Force (FATF) observed, "Reliable digital ID can make it easier, cheaper and more secure to identify individuals in the financial sector." However, the FATF also cautioned, "Digital ID assurance frameworks and standards and anti-money laundering and countering the financing of terrorism (AML/CFT) regulations have different origins and intended audiences."[3] How Digital ID impacts the execution of these priorities is not central to this analysis, nevertheless, these two disciplines – Digital ID and AML/CFT are interconnected.

Potential technical solutions are offered and organized into three core processes: identification, authentication, and authorization. We explore the benefits and use cases of digital identity solutions and follow with a discussion of challenges and considerations.

Background

Digital ID is a digital version of a person's identity, containing information and data that uniquely verify an individual in the digital world. Customer Identification Program (CIP) components include name, physical address, date of birth, and tax ID. Verification includes processes to form a reasonable belief that the customer is who they say they are (not all 4 need to be verified) and can include documentary or non-documentary processes. Digital ID does not have to be singular, but rather there can be various versions of a person's digital presence, which can reflect someone's online behavior, e-commerce purchases, or digital formats of physical documents such as passports and drivers' licenses. A user's social media account or the information provided to an online store to make a purchase can all be part of a digital presence. Within payments and financial services, a digital ID serves to identify an individual making a payment or requesting a product or service from an online platform.

[1] Financial crime may include money laundering, terrorist financing, and fraud.
[2] Paul A. Grassi and James L. Fenton, "Digital Identity Guidelines," National Institute of Standards and Technology, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[3] Guidance on Digital ID

While the concept of digital ID is not new, some federal and state government agencies and providers of digital IDs have established frameworks for the public. The Transportation Security Administration (TSA) now offers the acceptance of a digital driver's license at TSA checkpoints in over two dozen states, allowing for user identity verification to be fully digital via credentials and biometrics.[5] The benefit, beyond convenience, is that only the necessary personal information is shared. Mobile ticketing apps, travel documents, and the usage of any digital wallet, which each require digital verification of a user and track a user digitally, are all forms of a person's digital ID.

Globally, several countries have begun offering a single digital ID that allows users access to payment and financial services. Singapore offers SingPass, a single-login authentication system that supports any physical ID or document within a centralized infrastructure. It covers 97 percent of Singapore's citizens and residents aged 15 and above,[6] and reportedly processes over 41 million transactions per month.[7] India offers a service called Aadhaar, a unique number that is connected to a person's biometrics, allowing government agencies and services to authenticate an individual's identity from anywhere.[8] Although it is reportedly not proof-of citizenship, it is required to receive welfare payments and social services.[9] India advocates for the program to enhance social and financial access and to increase convenience.[10] The Australian government implemented a voluntary, national digital ID system in early 2024 following two large data breaches. The digital ID system allows users to verify their existing documentation in one system.[11] As digital IDs develop globally, understanding the use cases, operational functionality, and risks remains essential.

SECTION 2 – BARRIERS TO PAYMENTS AND BROADER FINANCIAL ACCESS

The Federal Reserve Bank of Atlanta's report *Promoting Payments Inclusion in a Digital Payments Era* examines barriers to financial services. As payment options advance with innovations, this creates the potential of excluding vulnerable populations. The paper explores who these populations are and what challenges hinder their financial access. A few examples of those are 1) stringent documentation

[4] Concordium, "A Brief History of Digital Identity," Medium, November 2020, https://medium.com/concordium/a-brief-history-of-digital-identity-8c8c0b52e3be.
[5] Suzanne Rowan Kelleher, "TSA Now Accepts Digital IDs from These Nine States," Forbes, June 2024, https://www.forbes.com/sites/suzannerowankelleher/2024/06/12/tsa-digital-ids-nine-states/.
[6] Smart Nation Singapore, "Factsheet – Singpass (Singapore's National Digital Identity," Smart Nation Singapore, March 2022, https://www.smartnation.gov.sg/media-hub/press-releases/singpass-factsheet-02032022/.
[7] Singpass, "Your improved digital ID to make life easy," Singpass.gov, April 2025, https://www.singpass.gov.sg/main/.

[8] Unique Identification Authority of India, "One Aadhaar, "Government of India, March 2025, https://www.uidai.gov.in/en/286-faqs/your-aadhaar/aadhaar-features,-eligibility/1934-what-are-the-features-and-benefits-of-aadhaar.html
[9] Billy Perrigo, "India Has Been Collecting Eye Scans and Fingerprint Records From Every Citizen. Here's What To Know, "TIME, September 2018, https://time.com/5409604/india-aadhaar-supreme-court/.
[10] Kamakshi Ayyar, "The World's Largest Biometric Identification System Survived a Supreme Court Challenge in India, "TIME, September 2018, https://time.com/5388257/india-aadhaar-biometric-identification/.
[11] Department of Finance, "Australia's Digital ID system," Australian Government Department of Finance, December 2024, https://www.finance.gov.au/government/australias-digital-id-system.

requirements 2) lack of access to broadband or smart technology and 3) security and fraud concerns. Taken together, these circumstances complicate access to the financial system. Technology, including digital identification and verification, combined with expanded broadband, has the promise to address some of these barriers.

Stringent documentation requirements

Some customers may find it challenging to produce adequate documentation and authentication of personal credentials to open a transaction account. The World Bank Group's Identification for Development Initiative defines a credential as any document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. This can include non-digital and digital mediums. The 2021initiative estimates that roughly 850 million people in the world do not have an official form of identification, whether analog or digital.[13]

In the United States, financial institutions are subject to reporting requirements to prevent money laundering, fraud, and misuse of funds under the Bank Secrecy Act (BSA). Know-Your-Customer (KYC) is a process financial institutions use to verify an individual customer's identity. KYC standards help protect financial institutions, service providers, and consumers. The standards also help protect against fraud, money laundering, terrorist financing, and other criminal activities. The documents that satisfy KYC requirements can vary, but in the US, most financial institutions accept a driver's license, passport, or state-issued identification card. This includes conducting an assessment to determine the customer's identity and normal transaction behavior. Customer Identification Programs and Customer Due Diligence are statutory requirements and must be included in the foundational components of a financial institution's BSA compliance program. Core requirements include identifying and verifying legal entity customers and beneficial owners, creating risk profiles, and reporting suspicious transactions.

A common form of identification is a drivers' license; however, many Americans lack this basic documentation. According to a 2023 University of Maryland study, approximately 29 million US citizens did not have a current driver's license, and another seven million did not have any other current form of government-issued photo identification. When responses were separated by race, it was found that Black, Hispanic, and Native Americans were reported to be the least likely to have a current form of government-issued ID or driver's license. Respondents with lower education and income levels were also less likely to possess these forms of ID. Furthermore, those who identified as having a disability were more than two times less likely to have a current ID.[14] The common approach of requiring one or more forms of identification for opening an account can be a challenge to these vulnerable populations. Likewise, balancing the responsibility of adhering to statutory requirements and providing accessible

[12] Raphael Bostic, Lali Shaffer, and Jessica Washington, "Promoting Payments Inclusion in a Digital Payments Era," Federal Reserve Bank of Atlanta, December 2023, https://www.atlantafed.org/banking-and-payments/payments-access/publications/2023/12/01/Promoting-Payments-Inclusion-Digital-Payments-Era.

[13] Julia Clark, Anna Metz, and Claire Casher, "ID4D Global Dataset 2021: Global ID Coverage Estimates. Washington, DC: World Bank." Washington, DC: World Bank. License: Creative Commons Attribution CC BY 3.0 IGO. https://documents1.worldbank.org/curated/en/099705012232226786/pdf/P176341132c1ef0b21adf11abad304425ef.pdf

[14] Michael J. Hanmer and Samuel B. Novey, "WHO LACKED PHOTO ID IN 2020? An Exploration of the American National Election Studies," University of Maryland, March 13, 2023, https://www.voteriders.org/wp-content/uploads/2023/04/CDCE_VoteRiders_ANES2020Report_Spring2023.pdf.

services remains a challenge for financial institutions. The rules do allow for electronic credentials such as digital certificates if financial institutions can ensure the legitimacy of third-party authenticators.

Lack of access to broadband or smart technology

For digital identity options to be viable, customers need appropriate devices and networks available to them. Accessibility is the first step for broader financial wellbeing. Historically, access was measured by a financial institution's geographical footprint. To open an account or conduct complex transactions, a customer may have been required to visit a physical branch. Over the last decade, we have experienced a shift in how financial services are offered as brick-and-mortars close and financial services become further digitized.[15]

According to a 2024 analysis from the Federal Reserve Bank of Philadelphia, the financial crisis marked a turning point in growing bank closures, but the onset of the pandemic accelerated this trend.[16] Typically, a banking desert is a census tract without a physical bank branch within a specified radius from its population center or within the tract itself: two miles for urban communities, five miles for suburban communities, and 10 miles for rural communities. The Federal Reserve has developed a Banking Deserts Dashboard which depicts a map of banking deserts in the United States. [17] In conjunction with the dashboard data, the Philadelphia Fed's report analyzes branch closures by asset size and demographics. Overall, the number of bank branches declined by 5.6 percent from 2019 to 2023. It is estimated that 12.3 million people are living in banking deserts.[18] Banking deserts may disadvantage vulnerable populations, such as low-income, disabled, minority, and elderly households who are already less likely to have access to digital banking. According to the Feds dashboard, broadband may be difficult to access for residents in 39 percent of banking deserts.

For many consumers and businesses, access to broadband or the use of mobile technology is their primary or only way of accessing financial services. According to the American Bankers Association, 77 percent of respondents in their 2024 survey used mobile or online platforms to conduct their banking in the prior 12 months.[19] The Federal Communications Commission (FCC) tracks fixed and mobile broadband coverage in the US. Using their data, the FCC published a working paper focusing on mobile technology. The study looked at demographics, types of technology used, and broadband quality via

[15] Lali Shaffer, "Who Are the 12 million People Living in Banking Desserts?" Federal Reserve Bank of Atlanta, May 2024, https://www.atlantafed.org/blogs/take-on-payments/2024/05/13/who-are-the-12-million-people-living-in-banking-deserts.
[16] Aliana Barca and Harry Hou, "U.S. Bank Branch Closures and Banking Deserts," Federal Reserve Bank of Philadelphia, February 2024, https://www.philadelphiafed.org/-/media/frbp/assets/community-development/reports/banking-deserts-report-feb-2024.pdf.
[17] Banking Deserts Dashboard, Fed Communities, January 2025, https://fedcommunities.org/data/banking-deserts-dashboard/.
[18] Aliana Barca and Harry Hou, "U.S. Bank Branch Closures and Banking Deserts," Federal Reserve Bank of Philadelphia, February 2024, https://www.philadelphiafed.org/-/media/frbp/assets/community-development/reports/banking-deserts-report-feb-2024.pdf.
[19] Consumer Survey Banking Methods, American Banker, November 2024, https://www.aba.com/about-us/press-room/press-releases/consumer-survey-banking-methods-2024.

speed tests. Minorities are more likely to use older mobile technologies than newer long-term evolution (LTE) or Wi-Fi technology given data collected from internet speed tests.[20]

Security and fraud concerns

According to the 2023 Federal Deposit Insurance Corporation Survey of Unbanked and Underbanked Households, privacy and trust issues were included in the top reasons for why consumers did not have a bank account.[21] Consumers are often concerned with financial fraud and theft of personal data related to financial accounts. Federal Trade Commission data from 2024 showed that 40 percent or 6.5 million consumer reports were related to fraud. More specifically, consumers reported $12.5 billion in fraud losses, a $2.5 billion increase over the prior year. Identity theft was reported by approximately 1.1 million submissions through payments methods like cards and payments apps. [22]

Businesses are also affected by fraud. A fraud study by LexisNexis cited that 75 percent of respondent organizations in North America found it challenging to retain consumer trust due to an increase in fraud rates. The study also estimates that every dollar of fraud costs North American firms approximately three times the actual value.[23] While this estimate may include operational expenses, it does not include reputational damage and external resources (such as law enforcement) deployed to investigate matters. Synthetic identity fraud and identity theft are among the most common types of e-commerce fraud, according to their study. Unlike identity theft, where a person's actual data is used, synthetic identity uses a combination of personally identifiable details to fabricate a person or entity to commit a dishonest act for personal or financial gain. For example, a profile may be created that only contains partial actual data while the remaining minor details are false. The next section explores possible solutions and considerations to these barriers.

SECTION 3 – SOLUTIONS

Digital payments require a baseline level of trust between counterparties and intermediaries. To the extent digital identity solutions can increase trust by improving security, privacy, and compliance with laws and regulations, they can reduce risk and costs for financial intermediaries and make some payment transactions more economical from a business perspective. Below we review two core infrastructure components: identification and authentication, along with several potential uses of digital

[20] Judith Dempsey and Patrick Sun, "The Digital Divide in U.S. Mobile Technology and Speeds," Federal Communications Commission, December 30, 2020, https://docs.fcc.gov/public/attachments/DOC-369010A1.pdf.
[21] Federal Deposit Insurance Corporation, "2023 FDIC National Survey of Unbanked and Underbanked Households," November 2024, https://www.fdic.gov/household-survey/2023-fdic-national-survey-unbanked-and-underbanked-households-report.
[22] Federal Trade Commission, "Consumer Sentinel Network Data Book 2024," March 2025, https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.
[23] LexisNexis, "2023 LexisNexis® True Cost of Fraud™ Study: Ecommerce and Retail Report," 2024, https://risk.lexisnexis.com/-/media/files/financial%20services/research/lnrs-2023-true-cost-of-fraud-study-nam-retail-and-ecommerce-report-v2-nxr16348-00-0224-en-us.pdf.

identity to expand access and improve quality of payment services for customers currently underserved by the market.

Greater accessibility to on-demand and self-service payment options depends on leveraging modern identity solutions and infrastructure. The most common digital identity solutions are often divided between identification and authentication solutions. For identification solutions, there are two primary forms of identification which include physical and digital. Some physical forms of identification include machine-readable or digital components. An example is an employee badge with a chip that holds a digital certificate or driver's license that includes a bar code or QR code with digitally signed information. Digital identification is often tied to a unique identifier such as a username, user id, or a digital certificate. Financial organizations often leverage physical identification to create an account and then issue digital identification for customers to access their account.

According to the World Bank, "As societies become more digital, we have begun to see a move toward digital-only ID systems that do not rely on the possession of a physical credential." [24] Identity is a component of the Digital Public Infrastructure (DPI). A key component to leverage identification across national, local, and digital boundaries is participation in a legal framework. "DPI are the digital platforms including the institutional and legal frameworks around them that enable the provision of essential society-wide functions and services. This typically entails platforms for identification and authentication […]. Their transformational potential in today's digital age can be likened to the way roads, railways, and other physical infrastructure fueled economic transformation in previous centuries."[25] Common legal framework standards or resources for identification and authentication include the European Union Electronic Identification, Authentication and Trust Services, the International Civil Aviation Organization, and Certification Authority Browser Forum for website digital certificates. The image shows common forms of identification and authentication, and how they are aligned to common financial access use cases.

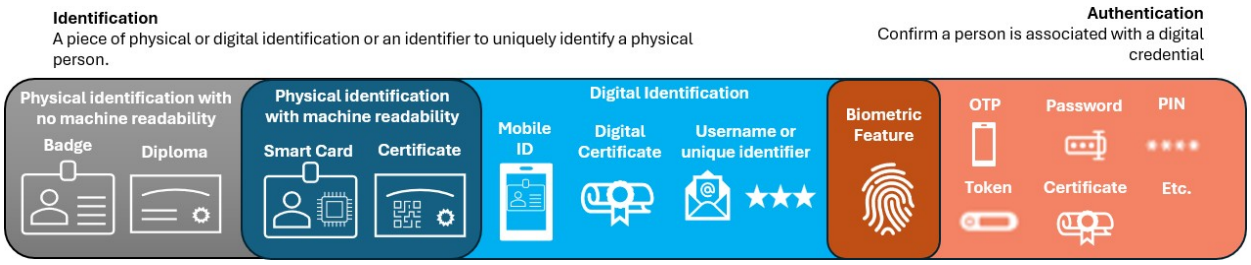

Figure 1. Example of identification and authenticators commonly issued by ID systems[26]

Authentication is the process of someone confirming their ownership over a digital credential using an authentication factor. There are three recognized authentication factors:

[24] World Bank Group, "ID4D Practitioner's Guide (English). Identification for Development Washington, D.C.", June 2019, http://documents.worldbank.org/curated/en/248371559325561562
[25] World Bank Group, "Identification for Development (ID4D) and Digitalizing G2P Payments (G2Px) 2022 Annual Report (English)", February 2023, http://documents.worldbank.org/curated/en/099437402012317995
[26] World Bank Group, "ID4D Practitioner's Guide (English). Identification for Development Washington, D.C.", June 2019, http://documents.worldbank.org/curated/en/248371559325561562

1 Something you know. A piece of static knowledge such as a password, PIN, or answer to a security question
2 Something you have. This is usually a physical device such as a mobile phone, a badge, or a USB key
3 Something you are. This is usually a biometric feature such as a fingerprint, eye, voice, or face, but can also be a modality such as typing speed, walking style, or clicking speed

As the threat of account and authentication compromise continues to grow, regulatory bodies are starting to use multi-factor authentication (MFA) over just a single factor such as password only. It is best practice to allow a user to register more than one authentication factor including a stronger phishing-resistant factor such as a Fast Identity Online (FIDO) passkey.

A passkey is a new way to sign in to applications or websites using the same process that unlocks a device (biometrics, personal identification number (PIN), or pattern), backed by public key cryptography. They are meant to replace passwords and are available on recent consumer devices and common web browsers using platform authenticators that come standard on laptops, workstations, and mobile devices. They can be synchronized on multiple devices using a cloud service. FIDO2 security keys are universal serial bus (USB) hardware devices that can also store passkeys and are another option that would not be tied to a specific smartphone or computer.

A review of identification and authentication methods and use cases

Identification process

Identity proofing first requires a unique physical person to be associated with a digital credential. Identity proofing can be accomplished through a three-step structure:

1. Resolution: The individual submits evidence and core identity information such as legal name and other required attributes to uniquely identify themselves.
2. Validation: The financial institution confirms the physical person exists, is unique, and that the presented evidence is authentic and accurate.
3. Verification: The financial institution verifies that the user is the owner of the identity evidence.

A financial institution can perform the identity proofing process in the following ways:

- In-person, if the individual has proper documentation.
- Remote identity proofing, which may rely on a selfie match to a form of photo identification.
- Supervised remote identity proofing follows the same process of remote identity proofing, but the session is supervised by a trained individual.
- Vouching involves a person or organization declaring they know the person is who they claim to be.

Identification use cases

Cross-border remittances: A key characteristic of remittances is the potential of high fees based on the use of multiple financial intermediaries, cost of leveraging global payment networks, and compliance costs and risks related to KYC requirements. Verifiable Digital Credentials, sometimes called Web3

credentials (used in combination with digital wallet), is gaining traction as a low cost and compliant digital identity solution to both strengthen the security and lower the cost of cross-border remittances.

Remote bank account openings: Several states in the US are piloting digital IDs or mobile driver's licenses, which may be stored in the digital wallet of a mobile device. Roughly half the states in the US are researching mobile licenses. This and other forms of digital identity and verification may create more opportunities for consumers to authenticate their identities. One of the growing threats with remote digital services involves identity fraud that leverages synthetic identities as well as deep fakes. One method to mitigate these attack vectors is ensuring that any piece of identification used to validate an identity is verified with an authoritative source.

Authentication process

Authentication establishes confidence that a physical person is associated with a digital account by validating credentials that are associated (bound) to their digital identity during and after identification. Examples may include the identifier associated to the account, password, fingerprints, other biometrics information, or passkey. Overall, not all forms of authentication provide equal strength and security. More organizations rely on requiring someone to authenticate with MFA. The most common MFA used for customers is a password and one-time PIN (OTP) for mobile applications. A stronger form of MFA gaining traction is a FIDO security key or passkey.

Authentication use case

Verifying public benefits: For the same reasons digital ID solutions might drive access and more affordability in remittances, they can also help improve the distribution of public benefits using digital payment rails. Requiring variable forms of MFA to perform different processes is a growing best practice. For example, authenticating an account may require any type of authorization while changing payment information or personal data would require a stronger form of MFA such as a passkey or security key.

While recent innovations enable more efficient, convenient, and secure forms of identification through digital means, public institutions remain the most critical provisioners of identity. Whereas private sector firms and Web3 can grant individuals credentials that are useful in specific contexts and shareable in their use across the internet, neither space has the authority to provision or originate one's actual identity in terms of establishing their name, date of birth, and foundational characteristics of their distinct "selfhood". How individuals exist in terms of government records like birth certificates, social security cards, passports, ID cards, and drivers' licenses are what legitimizes one's use of a name and identity in official interactions. No alternative is as trusted nor necessary in modern social structures. Therefore, the rate at which state and federal governments adopt digital identity protocols is likely the limiting factor for how quickly the public can realize the benefits of private sector innovation in this space.

Potential benefits to financial access

Digital ID solutions can support access to financial services in several complementary ways:

- Driving down the cost of KYC processes while improving their effectiveness can improve the economics of lower-value products and services like remittances or small-dollar loans which can increase access and affordability of financial services. Digital ID solutions may also enable efficiencies such as re-using KYC data created by other trusted parties.

- New privacy-enhancing technologies like mobile driver's licenses and Verifiable Digital Credentials allow someone to share only the information needed during credential presentation, thus reducing the risk of fraud and misuse of information.
- Digital ID solutions may also enable customers to compare offerings in the open banking system of the future, permitting their personal financial data to flow between trusted intermediaries who may offer better products and services than their existing provider.

SECTION 4 – RISK MANAGEMENT CONSIDERATIONS

These emerging digital identity solutions must manage three sets of risks simultaneously within an increasingly digital financial system: 1) an expanding threat environment with more sophisticated actors 2) new technologies which may come with steep learning curves for bank risk managers, cybersecurity teams, and compliance officers and 3) increasing reliance on a range of third parties like specialized vendors or customer-facing fintech firms who must support financial service providers' KYC compliance.[27] Managing these risks requires a comprehensive understanding of AML/CFT and cybersecurity risk management processes. It also creates new challenges for financial regulators and supervisors who generally focus on issues of customer identity through the lens of compliance with BSA/AML requirements.[28]

The evolving threat environment

The COVID-19 pandemic saw both an increase in digital payments usage and fraud, and these trends have continued to the present. [29] In 2023, nine out of ten consumers reported using "some form of digital payment over the course of the year" according to McKinsey research.[30] At the same time, the threat environment is increasingly characterized by sophisticated online actors leveraging a variety of tools, from synthetic identity fraud to generative AI. These crimes are often tracked by various entities.

- US Treasury's Financial Crimes Enforcement Network (FinCEN) found that approximately 1.6 million or 42 percent of total BSA reports and equivalent to $212 billion in suspicious activity, were related to identity in a review of BSA regulatory reports covering the full year 2021.[31]

[27] These long-standing regulations are intended to "properly identify persons conducting transactions and maintain a paper trail by keeping appropriate records of financial transactions;" KYC processes support law enforcement and regulatory agencies in pursuit of a variety of "criminal, tax, and regulatory violations." See FFIEC BSA/AML Manual; Existing guidance for bank examination staff in this area was developed in collaboration between federal and state banking agencies as well as the US Treasury Department's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Asset Control (OFAC).

[28] Other areas that may intersect with customer identity include compliance with consumer protection laws and regulations and credit risk assessments.

[29] During the pandemic, the role of cash decreased while credit card usage increased according to the Federal Reserve's 2024 Diary of Consumer Payment Choice.

[30] McKinsey. Consumer digital payments: Already mainstream, increasingly embedded, still evolving. McKinsey 2023 Digital Payments Consumer Survey.

[31] FinCEN. Financial Trend Analysis: Identity-Related Suspicious Activity: 2021 Threats and Trends. January 2024.

- Between March 2020 and June 2023, "at least 1,399 individuals or entities were found guilty or liable for fraud-related charges in cases involving federal COVID-19 relief programs."[32]
- The US Federal Reserve estimated that synthetic identity fraud cost US lenders $6 billion annually as of 2019, with more recent estimates suggesting the cost could range from $20 to $40 billion.[33]
- Contributing to this problem is the knock-on effects of cybercrime. According to the Identity Theft Resource Center's 2023 Annual Data Breach Report, data compromises increased by 78 percent in 2023.[34]

Thinking through risk management processes

These trends have highlighted the challenge of KYC and BSA/AML compliance in a digital financial system with greater need for remote account openings and digital transactions. Banks and supervisors need to understand the risks of digital identity and related technologies for financial institutions. Particularly as government-issued mobile driver's licenses become more commonplace, banks will become an integral part of the digital identity ecosystem. Certain digital ID solutions, like vouching, may even lead banks to serve as digital identity providers (as evidenced in Nordic countries).[35] As the federal financial regulatory agencies responsible for BSA/AML supervision have noted, digital ID innovations "can strengthen BSA/AML compliance approaches, as well as enhance transaction monitoring systems…to further efforts to protect the financial system against illicit financial activity [and] maximize utilization of banks' BSA/AML compliance resources."[36] There are, of course, risks associated with these technologies, including the quality of data inputs used in model training and development.

Digital ID's have the potential to streamline AML/CFT processes by utilizing technologies such as biometrics and electronic databases, thereby improving the accuracy and efficiency of identity verification.[37] The Financial Action Task Force (FATF) has offered specific guidance on digital identity: "using reliable, independent source documents, data or information…that provide an appropriate level of trustworthiness."[38] The FATF guidance advocates a risk-based approach, recommending that supervised institutions evaluate inherent risks of digital identity at every stage of the identity verification process. This involves robust record keeping and ensuring digital identity systems are reliable and independent.

[32] Government Accountability Office. COVID-19: Key Elements of Fraud Schemes and Actions to Better Prevent Fraud. October 19, 2023.
[33] See Federal Reserve, Synthetic Identity Fraud in the U.S. Payment System, Payments Fraud Insights, July 2019; Tad Simons, Trends in synthetic identity fraud, Thompson Reuters, April 21, 2023.
[34] Identity Theft Resource Center. ITRC 2023 Annual Data Breach Report.
[35] See, for example, Sweden's BankID, which can be used across digital society. BankID, Digital ID Card.
[36] Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (fincen.gov)
[37] Verification of customer identity through documents is a critical requirement of BSA/AML compliance under the Customer Identification Program (CIP) rule (see FDIC, Customer Identification Program), which notes that most individual customers may use "unexpired government-issued form of identification evidencing a customer's nationality or residence and bearing a photograph or similar safeguard" (e.g. a driver's license or passport). The CIP rule does allow for other forms of identification "if they enable the bank to form a reasonable belief that it knows the true identity of the customer."[37] A government-issued mDL, as outlined in Section 3: Solutions, would generally meet the above criteria, for example.
[38] FATF, Guidance on Digital Identity (2020).

Relatedly, these systems must also ensure a secure-by-design mindset to protect against identity theft and fraud. The National Institute for Standards and Technology (NIST) guidelines provide a framework for authentication and lifecycle management, emphasizing the need for secure binding credentials to verified identities.[39] Additionally, compliance considerations include ensuring that digital identity systems align with data protection and privacy regulations, necessitating cooperation between AML/CFT compliance teams, IT, and cybersecurity teams within an institution. Cybersecurity risks are further significant, as digital identity systems usually operate over open networks, making them susceptible to cyberattacks and identity theft. Financial institutions must optimize their existing cybersecurity controls and risk management processes.

SECTION 5 – SUMMARY AND CLOSING

Financial access remains a priority for the Federal Reserve. As financial products and services become more digital, the Fed aims to stay abreast of digital innovations to ensure that payments and financial services remain equitable, accessible, safe, and efficient. By exploring use cases and potential solutions, this report aims to better understand how digital identity could support financial access.

Digital IDs could help streamline AML/CFT processes, decrease costs around fraud prevention and monitorization and KYC processes, and enhance privacy and security. Future open banking systems may also benefit, allowing customers to utilize their digital ID within the market. A digital ID could help decrease remittance costs associated with KYC requirements in cross-border payments, which remain high for users. Additionally, the use of digital IDs on digital payment rails could remove costly intermediaries, making payments more direct, accessible, and affordable.

Digital identity can only be as successful as the parameters set around them to ensure safety, efficiency, and privacy in each use case. Even with increased fraud protection, vulnerable communities can still be targeted for data and identity breaches. Challenges with access may still exist, including digital divides, authentication barriers, or public concern regarding biometric data. Digital identities and digital payments require a baseline level of trust. If there's a lack of trust, then a service or solution would lack reliability by users.

Despite the concerns, digital identity solutions may gain trust from users and providers by improving security, ensuring compliance with standards, and reducing costs. As complexity increases in the financial services ecosystem, ensuring that every consumer and business in the US has access remains the goal. The implementation of innovative technologies, such as digital IDs, may reenforce the path to success.

[39] See National Institute of Standards and Technology. Digital Identity Guidelines (Second Public Draft, August 2024).