FinRegLab

Innovations for Identity Proofing and Transaction Monitoring

Advancing Financial Inclusion through Data and Technology

MARKET CONTEXT REPORT
OCTOBER 2024

About FinRegLab

FinRegLab is a nonprofit, nonpartisan innovation center that tests new technologies and data to inform public policy and drive the financial sector toward a responsible and inclusive financial marketplace. With our research insights, we facilitate discourse across the financial ecosystem to inform public policy and market practices.

Acknowledgments

Many of the insights in this report were derived from interviews with stakeholders in the financial services, technology, and civil society sectors, as well as a convening that FinRegLab held jointly with the Aspen Institute's Financial Security Program (FSP) in October 2024. FinRegLab would like to thank stakeholders who participated in interviews and discussions, Aspen FSP, and Visa for providing support for the convening. More information can be found on the inside back cover.

We would also like to thank individuals who provided valuable feedback on this report. They include:

Susana Barragán, UnidosUS
Nick Bourke, Consultant
Jeremy Grant, Venable LLP
Linda Jeng, Digital Self Labs LLC
Ivo Jeník, Consultative Group to Assist the Poor (CGAP)
Laura MacCleery, UnidosUS
Amit Sharma, FinClusive

Lastly, we would like to acknowledge the FinRegLab team for their work in writing this report:

David Ehrich, Gillous Harris, Abdulla Tarabishy, and Kelly Thompson Cochran

CONTENTS

1. EXECUTIVE SUMMARY

The ability to identify individuals both in person and online is fundamental to financial inclusion. However, 850 million people worldwide do not have official proof of identity.[1] In the US, roughly 35 million adult citizens either lack both current driver's licenses and state-issued identification cards altogether or have ones that list incorrect names or addresses, which can make it difficult to open accounts at banks and other financial institutions (FIs),[2] and the lack of trustworthy digital ID creates challenges for millions of consumers in online settings.[3] Consumers who are able to open transaction accounts can also face downstream difficulties in authenticating their identities and the legitimacy of individual payments, which may prompt financial institutions to decline transactions, freeze funds, and even close accounts due to erroneous concerns about suspicious activity.[4]

At the same time that "identity gaps" are creating roadblocks to financial inclusion for millions of consumers and small businesses,[5] large data breaches and other identity challenges are also making it more difficult for FIs to combat true bad actors.[6] Reports to the federal government of consumer fraud losses and identity-related suspicious activity have more than doubled since the pandemic,[7] but data limitations and other constraints are making it difficult for FIs to keep up. Fraud and scams also damage the financial stability and inclusion of vulnerable and historically underserved consumers, for instance by wiping out their savings and damaging their credit reports via identity theft.

The rapidly increasing cost of fraud and scams is prompting financial services providers to make substantial investments in new data sources, artificial intelligence (AI) tools, and data sharing infrastructures. These initiatives have injected new momentum into improving identity proofing and transaction monitoring solutions at a time when efforts to develop comprehensive frameworks for digital identity systems and data protection regulations in the US have been struggling to move forward. However, while data and technology innovations could create opportunities to advance financial inclusion and consumer privacy in addition to combating bad actors, they could also create risks of unintended consequences particularly for vulnerable and historically underserved consumers.

FinRegLab is exploring these issues to assess the potential value of conducting empirical tests and other research to analyze particular data and technology solutions for identity proofing and transaction monitoring. Toward that end, this paper surveys the financial services landscape to highlight proofing and monitoring gaps that impact financial stability and inclusion among vulnerable and historically underserved populations, as well as the potential benefits and risks of new data, technology, and process developments. It reflects interviews with dozens of individual stakeholders as well as collective insights from a convening held jointly with the Aspen Institute Financial Security Program in October 2024.

Specifically, the paper considers three contexts in which identity proofing and transaction monitoring can play a critical role in financial access: account opening, processing domestic transactions, and cross-border payments. It also considers three emerging data and technology developments for verifying and authenticating customer identities, monitoring transactions, and combating bad actors:

- Leveraging more diverse data sources, such as data collected from digital activities and users' devices;
- Applying more sophisticated analytical techniques to identity proofing and transaction monitoring systems, for instance to detect attacks that use generative AI to bypass online identity verification; and
- Using data sharing platforms and privacy-enhancing technologies (PETs) across institutions and jurisdictions to improve the accuracy of initial identity verification and ongoing client, transaction, and fraud monitoring models.

As fraud and scam defense draws more attention, the paper concludes that sustained engagement by policymakers, industry, advocacy, and research stakeholders could help to ensure that new data and technology initiatives are structured in ways that *also* help to close existing identity gaps, build long-term digital infrastructure, and reduce the risk of substantial unintended negative impacts on consumers and smaller institutions. The paper highlights the potential value of public empirical research, initiatives to reduce cost and efficiency frictions, and addressing emerging policy questions as stakeholders continue to work toward developing broader frameworks for digital identity and data protection. Such initiatives could include:

- Mapping US identity gaps at account opening as well as the extent to which weaknesses in downstream authentication and transaction monitoring have significant impact on consumers' financial stability and access to financial services.
- Empirically evaluating non-traditional data sources, advanced analytics, and data sharing tools for their impacts on accuracy, financial inclusion, and consumer privacy.
- Reducing cost and efficiency frictions that can discourage financial institutions from adopting more inclusive practices, for instance by supporting efforts to standardize security elements for different types of government-issued IDs, expanding upon current mobile driver's license initiatives, and improving systems for issuing, validating, and using Social Security Numbers and Individual Taxpayer Identification Numbers.
- Tackling a range of emerging policy questions regarding legal and regulatory expectations, collective action challenges, and how to strengthen FIs' incentives to invest in systems improvements. These include:
  - Whether and how to reduce current restrictions on and disincentives for financial system stakeholders to engage in data sharing in light of the increase in fraud and scams, and the efficacy of PETs to address privacy and confidentiality concerns while facilitating strategies to improve model performance.
  - Whether and how federal consumer financial laws, model risk management guidance, and responsible AI principles should be applied to anti-money laundering (AML) and anti-fraud activities in light of law enforcement concerns and escalating customer losses, and the efficacy of various data science techniques in meeting regulators' expectations with regard to efficacy, explainability, fairness, and other compliance concerns.

- Whether and how to strengthen positive incentives to encourage FIs to invest in more inclusive identity proofing and transaction monitoring practices to improve access for populations that may be relatively unprofitable to serve, for instance by providing credit under the Community Reinvestment Act.
- How to manage gaps in information access and technology resources among smaller banks that make it more challenging for them to keep up with market developments and best practices, potentially creating risks for both the institutions and their customers.
- The need for additional strategies for combating scams in which consumers are tricked into authorizing fraudulent transactions, including the efficacy of education initiatives, coordination with social media and telecommunications providers, potential revisions to legal frameworks, and other approaches.
- What balances to strike with regard to security, convenience, and privacy in the context of faster payments systems and other evolution in payments channels.
- Whether risk-tiering of transaction accounts to allow access to basic banking services could provide a viable inclusion strategy in the US, either in its own right or as a supplemental safeguard when testing less traditional data sources or other approaches to increase financial inclusion.

Identity proofing and transaction monitoring are increasingly urgent issues for industry, policymakers, advocates, and other stakeholders. Increases in fraud and scams are sparking substantial investments in data, technology, and process changes by some private market actors, but other stakeholders do not have visibility into these innovations. It is particularly important for policymakers to consider how smaller institutions and individual customers could be impacted by such changes. Broad and sustained stakeholder engagement is critical to both identify potential opportunities to structure these changes in ways that improve financial inclusion, security, privacy, and customer experience, and to mitigate risks of negative outcomes on markets and individuals. Particularly in the absence of comprehensive US frameworks for data protection and digital identity, fraud and scams defense initiatives may present the best opportunity to help improve identity infrastructures in the near future.

2. INTRODUCTION

The impacts of identity gaps on financial and broader economic inclusion have long been recognized as a substantial barrier to global development. Among the 1.4 billion adults worldwide (24 percent) that are estimated to lack accounts at banks or other regulated institutions, World Bank surveys suggest that about 27 percent lack identity documentation, rising to as high as 50 percent in some individual countries.[8] Overall, the World Bank estimates that about 850 million people (including both children and adults) lacked an official proof of identity as of 2021, with disproportionate impacts on residents of developing countries, women, and rural areas.[9]

Identity gaps in the United States are smaller but disproportionately affect certain communities. Among the 6 million US households (5 percent) that are estimated to lack accounts at banks or credit unions, federal surveys suggest that about 12 percent lack identity documentation needed to open accounts, including nearly 20 percent of unbanked Hispanic households.[10] Surveys of adult US citizens in the voting context find that about five million have neither a current driver's license (DL) nor an ID card issued by a state department of motor vehicles (DMV), which are the most commonly accepted forms of ID by financial institutions, and that another 30 million have DMV-issued IDs that do not reflect their current names or addresses. About three million lack *any* current form of government-issued photo ID.[11] Identity gaps are generally two to three times as common among Black, Hispanic, and Native American consumers as among White consumers, and they also disproportionately affect people experiencing housing instability, justice-involved individuals, victims of domestic abuse, transgender and nonbinary communities, and immigrant and low-income households more generally.[12]

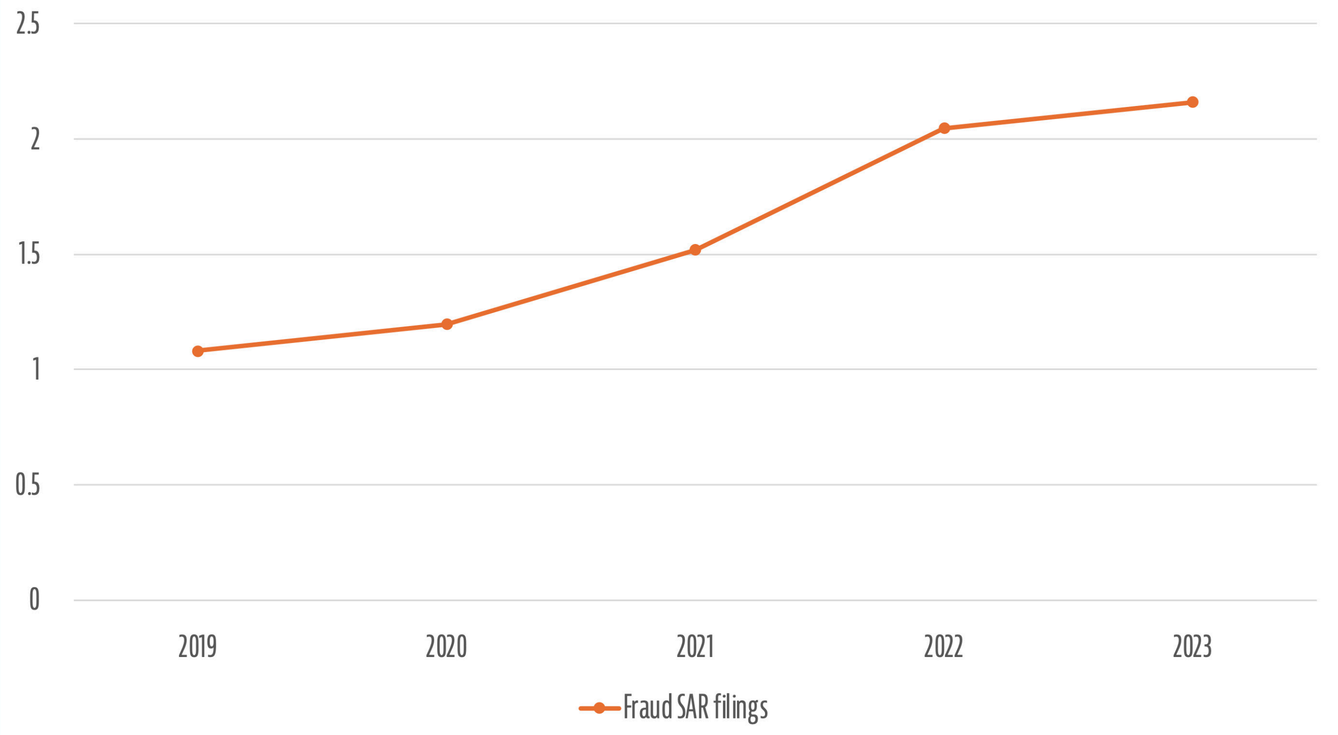
But lack of core government-issued documentation is only one strand of a broader set of challenges concerning proof of identity and the purpose and legitimacy of payments that can undermine financial access and stability among vulnerable populations. The increasing volume of online transactions has also increased the critical need for reliable forms of identification in digital settings, both in opening financial accounts remotely and in executing individual payment transactions. Large data breaches and bad actors' adoption of AI and other advanced technologies have also helped to fuel substantial increases in fraud and scams as well as ongoing concerns about money laundering. The Financial Crimes Enforcement Network (FinCEN) reports that 42 percent of Suspicious Activity Reports (SARs) filed by US financial institutions involved identity-related issues in 2021, totaling 1.6 million reports that involved $212 billion. While numbers for identity-related SARs in 2023 are not yet available, FinCEN has indicated that they are likely to have doubled in volume and value. The subset of fraud-related SARs also roughly doubled from 2020 to 2023, reaching 2.2 million.[13]

BOX 1 INCREASING FRAUD LOSSES

Only a small fraction of consumers who experience fraud are estimated to report their losses to government agencies, although those who do may also contact multiple offices.[14] As a result, it is extremely difficult to find comprehensive, consistent estimates for annual fraud rates across the US. However, government databases, consumer surveys, and stakeholder interviews all point to substantial increases since the pandemic.

For example, consumers reported to the Federal Trade Commission (FTC) over $10 billion lost to fraud in 2023, compared to $3.5 billion in 2020.[15] Nasdaq estimates that US financial institutions' 2023 losses to fraud totaled $127 billion and that scams cost American households and small businesses another $11.3 billion, with nearly 20 million households (15 percent) losing an average of $575.[16] The Global Anti-Scam Alliance estimates based on consumer surveys that fraud and scams cost $159 billion in 2023, affecting about 23 percent of U.S. consumers.[17]

FIs' reports of suspected fraud have also risen sharply since the pandemic. FinCEN reports that FIs filed about 2.2 million SARs for suspected fraud in 2023, compared to just under 1.2 million in 2020.[18]



Data Source: 2024 Report on Employer Firms: Findings from the 2023 Small Business Credit Survey (Federal Reserve Banks 2024)

Several trends are contributing to the escalation, including a significant jump in international fraud activity that focused initially on pandemic relief programs and has since shifted to other targets, ongoing increases in "synthetic identity fraud" often involving data elements that have been leaked in prior breaches,[19] and a surge in stealing and altering paper checks.[20] Digitalization of payments and banking is also contributing, as it is increasingly easy for consumers to authorize wire transfers and real time payments via phone apps and banking platforms. These channels are heavily used by fraudsters in part because it is more difficult to claw back funds after the fact.[21]

These challenges in proving consumers' identity and the legitimacy of their transactions can result in financial exclusion and impair affected households' financial stability. In some instances, FIs may consider consumers with more limited identity documentation and financial history to be too risky to serve, and in other cases the financial returns from serving these customers may not offset the incremental costs of implementing new and more expensive risk controls for both fraud and illicit finance. Increasing bad actor risk may lead FIs to further constrain their identification criteria, resulting in fewer people having access to financial services accounts, more people having their accounts frozen or closed, and more rejections or interruptions of legitimate transactions.

Banks interviewed for this project reported that they reject over 30 percent—and for some institutions as many as 90 percent—of new online account applications due to an inability to verify identity and the rise of synthetic identity fraud.[22] While data is spotty, some sources estimate that 15 percent of US consumers annually have transactions turned down or their credit card accounts frozen due to concerns about suspicious charges.[23] Recent news reports also suggest that account closures are rising because US financial institutions are relying more heavily on automated processes to respond to rapid increases in the volume of SARs filing since the pandemic. However, bank stakeholders dispute that such decisions are made without careful human review, and complaints about closures filed with the Consumer Financial Protection Bureau remain relatively modest.[24]

Financially vulnerable consumers can also be disproportionately affected where financial institutions' screening systems fail to detect fraud and scams. Even small dollar amounts can represent a significant percentage of monthly income or balance sheet savings for low- to moderate-income (LMI) households.[25] Various government and consumer advocate surveys have found Black and Latino consumers experience fraud at a higher rate than White consumers,[26] and the Identity Theft Resource Center reports that women and Black victims seek its assistance at higher rates than their proportion of the general population.[27] Where vulnerable consumers have been the subject of identity theft or scams and fraud, the damage to their finances and credit reports can further undermine their ability to access financial services in the future.

To address these concerns, financial system stakeholders are increasingly turning to more diverse data sources, advanced analytical techniques, and data sharing initiatives as a potential way to combat fraud and scams, improve the efficiency and effectiveness of existing processes, and increase inclusion. These innovations include broadening identity validation systems to rely on information from customers' digital footprints as well as increasing reliance on more sophisticated machine learning and AI models. Stakeholders are also exploring a range of PETs, such as encryption methods and federated learning models, to balance the potential benefits of exposing analytical models to more data with the risks to privacy and security of moving and consolidating large amounts of customer information.[28]

Depending on how these new data and technology strategies are structured and implemented, they hold both promise and peril. On the one hand, they could offer opportunities to mitigate bad actor risks while improving financial inclusion and/or customer privacy *at the same time*. On the other, they raise potential questions with regard to reliability, explainability, fairness, privacy, and security, as well as concerns about smaller financial institutions' ability to deploy such strategies. While fraud rates are driving significant investment by industry, it is important for the whole spectrum of stakeholders—including regulators—to engage on these topics, both to consider whether and how general tenets of consumer protection and responsible AI use should be applied in the context of defending against bad actors and to ensure that the potential benefits and risks to financial inclusion are considered carefully.

To inform such engagement, Section 3, Section 4, and Section 5 of this paper investigate three areas concerning how identity proofing and transaction monitoring can impact financial inclusion:

- Verification at account opening (e.g., "Are you who you say you are?"),
- Authentication and monitoring of domestic payment transactions (e.g., "Are you the account owner, and did you authorize this transaction for legitimate purposes?"), and
- Authentication and monitoring of cross-border transactions (e.g., "Can the sending and receiving parties be confirmed in both jurisdictions?").[29]

In each context, the sections summarize legal requirements and regulatory expectations, industry practices, and financial inclusion concerns. Section 6 details recent data and technology trends, while Section 7 analyzes potential initiatives that could bridge current knowledge gaps and improve conditions for particular subgroups. Sustained engagement by policymakers, industry, advocacy, and research stakeholders is instrumental to closing existing identity gaps, building long-term digital infrastructure for identity, promoting privacy and cybersecurity, and reducing the risk that new data and technology initiatives have substantial unintended negative impacts particularly on financially vulnerable populations.

3. IDENTITY VERIFICATION AT ACCOUNT OPENING

The identity proofing process in account opening determines whether a person can establish an ongoing relationship with a financial institution that provides continuing access to the financial system. As a result, this is the operational step with the most direct impact on financial inclusion.

While US regulatory standards provide FIs with some flexibility in how they verify customers' identities at account opening, FIs have historically relied heavily on driver's licenses, DMV-issued ID cards, and credit bureau data to verify consumers' biographic information and financial histories. These practices are driven by a number of factors, including a desire to reduce risks by staying within the boundaries of safe harbors, uncertainty about the potential tradeoffs of adopting more creative approaches, and cost considerations. However, traditional approaches have disadvantages in terms of inclusion and accuracy, as many consumers struggle to obtain DMV-issued IDs and data breaches have exposed many applicants' credit bureau data. While some governments are attempting to develop alternative ID forms that may be easier to obtain and a number of states are developing "mobile driver's license" (mDL) programs that could provide a form of digital ID for more secure identity proofing online, progress to date has been slow.

3.1 Legal frameworks

The legal basis for identity proofing requirements in financial services is laid out in the Bank Secrecy Act of 1970 (BSA) for anti-money laundering purposes and in BSA amendments from the USA PATRIOT Act of 2001 (the Patriot Act) for countering the financing of terrorism (CFT). In practice, these requirements also combat financial fraud. The BSA and implementing regulations outline FIs' Know Your Customer (KYC) obligations at account opening as well as ongoing customer due diligence (CDD) and transaction monitoring requirements, which are discussed in Section 4. Covered financial institutions include banks, money service businesses (MSBs), businesses supervised by state banking authorities, and more, but this section focuses on requirements for depository institutions and MSBs.[30]

The Patriot Act amended the BSA to mandate that FIs implement Customer Identification Programs (CIPs). CIP requirements establish baseline procedures for customer identity verification prior to account opening. Banks' CIPs must include risk-based procedures and collect at a minimum the customer's name, date of birth, address (or the address of another contact such as a homeless shelter or nonprofit agency), and a taxpayer identification number (such as the customer's Employer Identification Number (EIN), Social Security Number (SSN), or, for non-US citizens, an Individual Taxpayer Identification Number (ITIN) or a passport or other foreign ID).

Banks must then verify the provided information shortly after account opening. According to BSA, the bank's verification procedures must enable it to "form a reasonable belief that it knows the true identity of each customer."[31] Regulations defining banks' CIP requirements do not specifically preclude any particular verification methods, but note that CIP verification procedures "may include" use of an unexpired government-issued photo ID or comparing information provided with information from a consumer reporting agency or public database.[32] MSBs must also verify customer identity, but the regulations are not as specific in describing specific documentation or approaches.[33]

Lastly, bank and non-bank FIs, including MSBs, are required to cross-reference a customer's information with lists of sanctioned individuals and organizations from the Office of Foreign Asset Control (OFAC) at account opening and through the lifecycle of an account.[34]

3.2 Industry practices

While "identity proofing" is a common industry term, practitioners generally think in terms of "identity risk management" when managing workflows for verifying identity during account opening both in person and online. The current approach to identity verification and authentication is a probabilistic framework and vendors are clear to state that they are not guaranteeing identity, but rather trying to measure "what is the likelihood that the identity provided is correct?"

BOX 2 DATA TYPOLOGIES FOR IDENTITY

Historically, FIs have relied on government-issued physical identification cards and documents to obtain specific **biographic data**, such as name, address, date of birth, and social security number. Particularly in the online context, they have also often used **knowledge-based verification**, for instance by drawing on credit report data to ask applicants or customers questions about their past addresses or credit use as a way to validate identities.

Over the past two decades, **biometric data** such as fingerprints, voice imprints, iris scan, and facial recognition have increasingly been adopted by smartphone manufacturers, apps, and online identification platforms, and to a lesser extent by FIs. For example, in circumstances where a transaction appears suspicious, some FIs may conduct "liveness tests" that compare short videos of a customer to the images from their photo IDs.

More recently, FIs have begun confirming biographic data against a broader set of sources, such as wireless carrier records, and using a range of **behavioral data** particularly from digital activities. The latter approaches include analyzing data patterns about when, where, and how individuals use their devices, such as keystroke timing patterns and geolocational data.

BOX 3 GOVERNMENT VERIFICATION SERVICES FOR SSNs AND OTHER IDENTITY INFORMATION

Government agencies can play an important role in helping to verify different attributes that are used by financial institutions and other commercial actors to authenticate consumers' identities. For example, in an effort to combat synthetic identity fraud, Congress directed the Social Security Administration to set up the electronic Consent Based Social Security Number Verification (eCBSV) service to allow FIs that obtain consumers' consent to verify whether combinations of names, dates of birth, and SSNs match federal records. However, bank use has been affected by fee increases and relatively high mismatch rates that may prompt institutions to reject legitimate consumers who are not matched by the system due to nicknames, maiden names, or typos. To date, the SSA has declined to provide additional detail about no-match responses.[35]

The National Institute of Standards and Technology released a report in October 2024 that surveys the landscape of government agencies providing attribute validation services, which can be particularly helpful in verifying identity in virtual settings. The report provides nonbinding guidance on architecture, security, privacy, and operational considerations for government agencies that are seeking to create or improve verification services.[36]

FIs generally start by collecting an applicant's taxpayer ID number and biographic information, including name, address, employment, and date of birth. Online applications generally require email and phone verification as well, and they often require the applicant's consent for the FI to obtain information about the applicant and their device from their wireless carrier. FIs rely overwhelmingly on DLs or DMV-issued ID cards as part of their verification processes, running the cards through physical scanners when applications occur in person and collecting the ID number and often images of an ID from online applicants. FIs may also collect utility bills or other documents as additional proof of address. For both online and in-person applications, the FI may also verify the applicant's SSN electronically with the Social Security Administration (SSA) and/or pull identification data from credit reporting agencies.

FIs or third-party service providers then analyze the data collected from the consumer and other sources to determine the authenticity of data presented. They may additionally ask verification questions of the applicant based on data from credit bureaus or other sources. However, these traditional verification methods are becoming increasingly ineffective, as major data breaches have leaked vast quantities of personal information, exacerbating identity theft and account takeover among other vulnerabilities. Additionally, legitimate applicants often have difficulty remembering information for knowledge-based verification questions.[37] The authenticity of the identifying information provided is then risk-scored for comparison to thresholds that the FI has previously set to define which risk levels are subject to auto-accept or auto-reject decisions, or if they are "stepped up" to a more thorough manual review.

In some cases, when a FI cannot auto-accept a consumer's identity online, the consumer is instructed to visit a branch for in-person verification. For example, if an applicant does not have a phone number or does not have a credit file, FIs typically route them to a branch to verify their DL or state non-driver identification cards and supplemental documentation. Such practices create additional friction for certain customer groups, which can exacerbate dropout rates.

3.3 Financial inclusion concerns

Federal surveys suggest that about five percent of US adults and households have no checking or savings accounts.[38] Although respondents most frequently cite financial considerations such as minimum balance requirements and fees as reasons why they do not have an account, a significant proportion also cite lack of identity documentation (12 percent), mistrust in banks (33 percent), and privacy concerns (34 percent).[39] Surveys in both the banking and voting contexts suggest that lack of core identity documentation is disproportionately concentrated among Black and Hispanic consumers and low-income households,[40] and more specialized surveys and advocates also report high levels among unhoused people, victims of domestic violence, justice-involved individuals, and transgender and nonbinary communities.[41] The number of young people obtaining DLs is also declining, particularly in urban areas.[42]

Several factors can contribute to challenges obtaining commonly accepted ID, including:

- Some applicants do not have US birth certificates, including immigrants, a number of older Black adults who were born in Southern rural areas, and some older Native Americans born on tribal lands.[43]
- People facing housing insecurity often struggle to maintain identifying documents in acceptable condition. Laminating them can backfire because the documents may be rejected due to their altered format.[44]

- Cost, time, and geographic access challenges can make it more difficult for low-income and transportation-constrained populations to be able to obtain or renew identity documentation, especially where some states have closed DMV offices or restricted hours.[45] Circular requirements to present one type of ID to obtain another type of ID can also make it difficult to replace materials that have expired or been lost, stolen, or damaged.[46]
- Name spelling variations and other inconsistencies, omissions, or mismatches between records can prompt documentation to be rejected. However, obtaining corrections may be difficult for many of the reasons discussed above.
- Process challenges with regard to verifying SSNs and obtaining and verifying Individual Taxpayer Identification Numbers with the federal government and variances in state policies concerning transgender and nonbinary individuals and consumers with different immigration statuses can also complicate consumers' ability to satisfy FIs' identity documentation and verification requirements.

The fact that FIs focus so heavily on DLs and other DMV-issued identity cards also has inclusion implications. While the legal framework for CIP does not *require* a DL or a state-issued non-driver's license ID, common practice across FIs is to require current versions of these ID forms as the physical form factor used for identity proofing, especially in account opening.[47] Although FIs were more accepting of expired IDs during the early days of the pandemic, many have since tightened their practices to require current or only slightly outdated forms (e.g., within 30 days of expiration). In some cases, FIs further narrow the focus to require that a customer opening an account provides a current DL from a state representing the geographic footprint of the bank. These kinds of variations create additional uncertainty for consumers in seeking to open accounts.

BOX 4 DIFFICULTIES FOR ITIN HOLDERS

The Individual Taxpayer Identification Number (ITIN) was originally created by the IRS to allow foreign nationals who do not qualify for an SSN (both resident and non-resident aliens) to file taxes, with about 5.8 million ITINs active as of December 2022.[48] ITINs have taken on a broader identity role for many holders, a large proportion of whom are foreign nationals who lack authorization to stay permanently in the US.[49] Many banks, especially larger ones, accept ITINs in lieu of SSNs, allowing holders to access various financial services if they meet other KYC requirements.[50] Additionally, ITINs can be used to obtain DLs in many of the 19 states and the District of Columbia that have laws permitting immigrants who otherwise lack permission for permanent residency to obtain such licenses.[51]

Obtaining an ITIN in the first place can be difficult, however, as individuals must first receive enough income to file taxes and must then file paper returns. ITIN applications must also include ID, such as a valid foreign passport, to prove both their identity and their foreign status.[52] These original documents (or copies certified by the issuing agency itself) must typically be mailed to the IRS, meaning that applicants do not have their IDs while the application is processed (up to 14 weeks) and that they must have a reliable mailing address to receive their returned documents.[53] Applicants can avoid mailing documents by visiting a Certifying Acceptance Agent, but these agents frequently charge hundreds of dollars per application.[54]

After obtaining an ITIN, consumers often still face obstacles in obtaining financial services. For example, the Social Security Administration's eCBSV service does not provide electronic verification of ITINs. ITIN holders also frequently encounter challenges in the event that they later obtain an SSN. Individual lenders and consumer reporting agencies do not necessarily connect their files under the two numbers, and some consumers find that they effectively have to start over in building credit history. To the extent that credit report data is used for identity proofing in other contexts, this can have implications beyond credit access.[55] In the credit context, research by identity vendors suggests that ITIN holders who were granted credit cards and auto loans were often less likely to default than SSN holders with equivalent credit scores, even though many lenders have historically been reluctant to extend credit because of perceptions that such consumers are higher risk.[56]

BOX 5 THE FEDERAL REAL ID INITIATIVE AND THE STANDARDIZATION AND TIERING OF ID

While standardization of major ID forms across government entities can substantially simplify account opening processes for financial institutions, such initiatives in the US context can sometimes trigger tensions and coordination challenges with regard to privacy, security, and federalism. The REAL ID Act of 2005, which was adopted in the wake of the 9/11 attacks, illustrates many of these issues.

The law specifies standards for forms of identification that can be used to board domestic flights and enter certain federal and nuclear facilities, but it does not mandate that states use those standards in issuing IDs for other purposes due to substantial sensitivities about the prospect of creating a national ID system. Nevertheless, some states initially resisted developing bifurcated processes to allow individuals who can and want to meet the documentation standards to obtain REAL IDs. All states are now in compliance or operating under temporary waivers, and the current deadline is set for May 7, 2025—just shy of two decades after enactment.[57]

REAL ID outlines strong standards both for the physical security features on issued IDs and identity documentation and verification requirements during issuance.[58] The latter include required identity documentation and document validation procedures that are more intensive than many state ID programs.[59]

These strict issuance requirements make REAL IDs difficult to obtain, and they have in some ways led to a tiered identity system in the US where municipal and other alternative IDs are both less secure and less standardized than conventional DLs or state-issued non-driver ID cards, which are somewhat less secure and less standardized than REAL IDs. However, while REAL IDs are used to board flights and enter certain federal facilities, they are not required by financial institutions.

Examples of government-issued alternatives to these licenses could include:

- US passport or passport card
- US military card
- Permanent resident card
- State-issued prison ID
- State-issued gun license
- Municipal ID

However, many FIs do not accept alternatives to DLs as a primary ID for purposes of account opening. They point to both cost and risk considerations, given the increasing use and sophistication of counterfeit IDs and differences in the issuance processes and the physical security features of different types of ID. Current best practice involves use of onsite hardware “readers” with updatable software to confirm the authenticity of the presented ID, such that each type of ID accepted (e.g., DLs vs passports) may require additional software packages and in some cases additional machines. Other considerations include the need to train staff, high rates of staff turnover (e.g. between 20 and 40 percent annually),[60] and having to maintain multiple processes to verify different kinds of physical IDs. FIs often find it difficult to measure the tradeoffs between the cost of implementation, the potential for incremental fraud, and the positive impacts from increasing financial inclusion.

These dynamics have affected FIs’ willingness to accept IDs created by municipal governments such as New York City, which launched its program nearly a decade ago in an attempt to increase access to financial and other services.[61] Furthermore, while a number of countries have developed programs to offer simplified bank accounts to consumers who lack full traditional identity documentation, US programs focusing on basic banking accounts have never focused specifically on this population.

BOX 6 IDNYC

New York City's municipal ID program, IDNYC, has been one of the most successful efforts to help close identity gaps. Launched in January 2015, the program has grown to more than 2 million cardholders.[62] However, the program has not gained much traction among financial institutions.

State banking regulators have encouraged FIs to accept the ID in their customer identification programs,[63] and federal regulators have confirmed that the ID could be used to satisfy CIP requirement while noting that there may be higher risk cases where additional information about an individual applicant is required.[64] However, use by FIs has remained limited. Only a few small FIs in the city accept the ID as a primary form of identification, and most of these FIs are credit unions that have other requirements for membership.[65] PNC Bank will also accept it as a secondary form of ID.

In interviews, FIs that do not accept the ID primarily cited security concerns, including the number and quality of physical security features on the card, as well as the reliability of the underlying data used to issue the ID. FIs are concerned that IDNYC can be easily counterfeited, as it has few physical security features compared to state IDs.[66] Interviewees also were not convinced of the reliability of the information that is accepted for issuance. For example, a person claiming to have been born in the city can provide a letter of attestation from a homeless shelter, an employee ID card, and a school ID card to obtain an IDNYC card—all of which are much easier to obtain or counterfeit than a birth certificate or other documents required for state ID card applications.[67] Ultimately, accepting IDNYC as a primary form of identification would incur costs for FIs in terms of staff training and infrastructure to validate the ID and potentially expose them to an uncertain level of fraud risk, which may not be offset by the revenues from the customers in question.

BOX 7 TIERED ACCOUNTS AND BASIC BANKING PROGRAMS

While US financial institutions typically use similar baseline KYC processes for general consumer transaction accounts, a number of developing countries have adopted tiered systems for KYC and CDD depending on the parameters of the underlying accounts.[68] This approach helps individuals who lack full traditional identity documentation open simplified bank accounts that have various restrictions, such as monthly transaction volume limits, that make the accounts less appealing to actors engaged in illicit finance. A second variation allows the opening of accounts with minimal documentation but requires additional information to be submitted if account use exceeds certain parameters.

Such programs are often paired with government initiatives to move to digital delivery of benefits, which can also encourage the opening of accounts. For example, Mexico approved a tiered KYC system in 2011 under which individuals can open basic accounts with monthly transaction volume limits by providing only their name, date and place of birth, gender, and physical address, and migrated its public benefits programs from prepaid cards to the most basic tier of accounts. The country added 9.1 million deposit accounts in commercial banks in the first two years of the program.[69]

However, research is limited as to the extent to which consumers graduate to higher-tier accounts and can access more sophisticated financial services over time, which could increase the financial inclusion benefits to households and the economic benefits to FIs. Stakeholder interviews suggest that the extent to which consumers use simplified, lower-tier accounts for more than receiving benefits varies. Individuals may be more likely to use these accounts if they meet their needs and there is a clear pathway to graduate to higher tier accounts and other financial services such as credit. Where open banking regimes are in place,[70] account history at one FI could be accessed and considered by additional FIs to help consumers qualify for higher-tier accounts across the financial system. It is unclear how frequently this happens in practice, however.

In the US, the federal government made a large push to encourage consumers to open basic banking accounts in response to 1996 legislation that shifted federal benefit programs from paper checks to electronic payments,[71] and more recent initiatives such as the Cities for Financial Empowerment Fund's "Bank On" program have encouraged FIs to provide simplified, low-cost accounts to help consumers avoid paying high check-cashing fees, overdraft charges, and expenses for basic payment services.[72] Interest in offering bank accounts through the US postal system has also been raised periodically in Congress.[73] While many of these programs have explicit financial inclusion goals, they have not specifically focused on consumers who struggle to open accounts because they lack identity documentation.[74]

3.4 Mobile driver's licenses

In an effort to address the increasing demand for online digital verification, several states have started to issue digital versions of their DLs with the data elements that are present on a physical DL and a cryptographic signature rather than a simple and insecure digitized image. These mobile driver's licenses are stored in a mobile wallet or other app on a consumer's smartphone, which can in turn transmit the information to other parties' reading devices for authentication. As of August 2024, 27 states have mDL programs in some stage of development.[75]

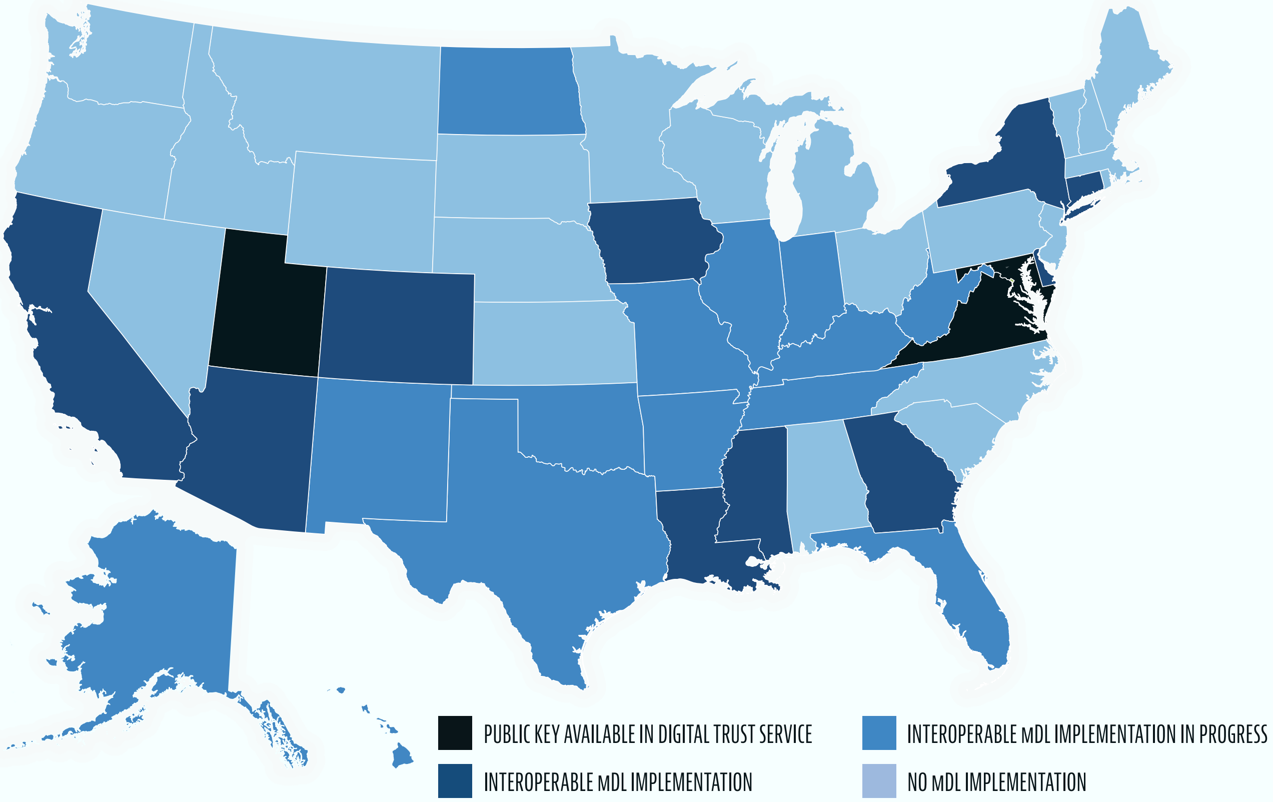
MDLs not only can be advantageous to consumers in renewing their credentials and dealing with situations in which their physical IDs are lost, stolen, or damaged,[76] but also offer the potential for more secure and efficient online identity verification and authentication. MDLs are secured using public key cryptography, a technology that makes counterfeiting, altering, or unauthorized use of an mDL extremely difficult. Public key cryptography is a class of cryptographic protocols whereby each mDL holder receives a publicly visible "key" that encrypts their information but cannot be used to decrypt it and is digitally signed to their mDL by the issuing authority. Each mDL user also receives a private key that can be used to decrypt information encrypted with the public key such that the private key never leaves the user's device. This method ensures that mDLs' digital signatures are verifiable and secure even in virtual settings where pictures or videos of physical ID can be faked.[77]

MDLs can also offer privacy advantages in situations in which only one aspect of an individual's identity needs to be verified, such as whether a consumer is over the age of 21 for the purchase of alcohol, since an application or wallet holding the mDL can be configured to transmit only the required information rather than the ID's full set of data elements.

MDLs are not being used today to replace traditional physical IDs, but rather primarily as a digital "backup" version of the state ID that can be presented to physical ID readers in such locations as stores or airports. For in-person use cases, the International Organization for Standardization (ISO) published standards for interoperability in 2021 (ISO/IEC 18013-5),[78] and the American Association of Motor Vehicle Administrators (AAMVA), an association of DMV administrators, is driving their adoption in the US and Canada. Figure 1 shows the varying levels of mDL adoption and adoption of the ISO/IEC 18013-5 standards across states. The Transportation Security Administration is also working on various initiatives relating to airport usage.[79]

Implementation initiatives for remote presentation of mDLs in online settings have proceeded more slowly but are expected to accelerate in fall 2024 as the ISO plans to formally publish a standard for remote presentation (ISO/IEC 18013-7)[80] and the National Institute for Standards and Technology (NIST) begins building a "reference implementation" focusing specifically on use of mDLs by FIs for online account opening, authentication, and step-up verification.[81] The latter initiative by NIST's National Cybersecurity Center of Excellence (NCCoE) involves working with 15 technology providers and industry actors including JPMorgan Chase, Wells Fargo, US Bank, and Block, to help build connections that the participating FIs could use to access mDLs via their mobile applications or through a browser on a consumers' smartphone or desktop computer.[82] NIST is also coordinating with federal regulatory agencies in hopes of using the project both to demonstrate how FIs can use mDLs at a technical level and to provide a compliance overlay regarding their utility for CIP requirements, as stakeholders report that some FIs are concerned about whether it is permissible to rely on such credentials absent more explicit guidance from regulators.

FIGURE 1 mDL IMPLEMENTATION AND DIGITAL TRUST SERVICE PARTICIPATION


PUBLIC KEY AVAILABLE IN DIGITAL TRUST SERVICE
INTEROPERABLE mDL IMPLEMENTATION IN PROGRESS
INTEROPERABLE mDL IMPLEMENTATION
NO mDL IMPLEMENTATION

Note: The mDL Digital Trust Service is a newly released service by AAMVA that facilitates interoperability by maintaining a collection of states' public keys used to authenticate mDLs.[83] "Public Key Available in Digital Trust Service" represents the highest level of interoperability in the map above.

Source: "Jurisdiction Data Maps - American Association of Motor Vehicle Administrators - AAMVA."

While the NIST initiative could help answer critical threshold questions for FIs, the strength of their incentives to invest in mDL implementation will also depend on broader market dynamics. For instance, some early state programs are prioritizing the use of open source wallets or apps to hold their mDLs in an effort to discourage proprietary wallets from imposing restrictions or charging for access. More broadly, the development of other use cases that drive consumer takeup rates would help to strengthen incentives for FIs and other companies to adjust their systems, creating network effects that increase mDL usage overall. Toward that end, the NIST NCCoE is also planning reference implementations focusing on federal agency programs and healthcare applications over two years.[84]

While mDLs do not address the most fundamental financial inclusion barriers facing consumers who lack current DLs or other government-issued ID in the first instance, they could become an important mechanism for opening and using online financial accounts and engaging in various other types of digital economic activities. Accordingly, they may still have important financial and economic inclusion implications, particularly for consumers who may lack access to smartphones and digital connectivity even if they have traditional physical identification documentation. Proactive engagement could help to reduce the risk that mDL systems exacerbate existing identity challenges. For example, the proposed Improving Digital Identity Act of 2023, which supports state mDL programs initially included supplemental funding to address the more basic identity challenge of helping individuals obtain underlying documentation to obtain DLs in the first instance. This provision was removed in the Senate, however.[85]

BOX 8 OTHER EFFORTS TO DEVELOP MORE COMPREHENSIVE DIGITAL ID FRAMEWORKS

Discussions of the need for comprehensive digital ID infrastructure have been increasing over the past decade across a broad range of sectors as a means of improving cybersecurity, improving AML/CFT and anti-fraud measures in payments, enhancing inclusion and user experiences, and facilitating cross-border payments.[86] In addition to government-issued digital ID initiatives such as mDLs, a number of consortia, non-profits, and companies are focusing on the use of distributed ledger technologies, as discussed further in Section 6, and technical standards established by the World Wide Web Consortium (W3C) to facilitate the creation of digital identifiers and verifiable credentials containing additional information or attributes. These identifiers and credentials can be used for several purposes, such as verifying professional memberships as well as elements of core identity.[87]

Adoption of these approaches is more widespread in other sectors than in financial services. However, some FIs have begun to use these technologies for limited applications, and stakeholders are working to organize additional initiatives.[88] Advocates believe that networks based on these systems could allow for "reusable KYC." In this system, consumers could provide a verifiable credential containing their identifying information, which has been verified by a trusted FI, in connection with real-time payments and when they access financial services from new providers. This would allow for near-instantaneous KYC. However, like mDLs, the usage depends on both regulatory acceptance and general adoption rates.[89]

As stakeholders in financial services and other sectors consider these initiatives more broadly, there are a range of views about the extent to which comprehensive digital ID platforms should be based on government-issued ID and how government and private entities should work together to foster broader trust networks for digital activity. Some advocates who are concerned about the vulnerabilities of centralized systems and/or governmental abuses envision "self-sovereign" systems where identity could be proven by an individual through attestations without relying on government-issued ID as a component.[90] However, governments have a strong preference to rely on their own identity systems in connection with taxing individuals and entities, providing access to benefits, and preventing illicit finance. Some stakeholders also raise concerns about identity data being potentially controlled by large private technology enterprises looking to monetize the information. Some countries and stakeholders have focused on public-private partnerships as a hybrid approach.[91] Consortia are also being formed to standardize processes around the issuance, verification, and revocation of digital credentials with both public and private sector participants.[92]

4. IDENTITY AUTHENTICATION AND MONITORING OF DOMESTIC PAYMENTS

While account opening is the identity proofing process with the greatest direct impact on financial inclusion, challenges in authenticating customer identities and monitoring both domestic transactions and cross-border payments (as discussed in more detail in Section 5) also have important implications. Where AML or anti-fraud systems erroneously flag legitimate transactions as suspicious (often called "false positives"), the transactions may be slowed, blocked, and/or reported to the government. Particularly in the AML context, financial institutions may choose to close underlying accounts where multiple flags accrue. At the same time, where FIs fail to detect and prevent transactions involving fraud and scams ("false negatives"), consumers can lose money, suffer credit report damage, and find it more difficult to access financial services in the future. FIs absorb a significant portion of fraud losses where various laws limit consumer liability, but experiencing fraud can still take a significant emotional toll on consumers and the cumulative losses can affect the scope and price of services that FIs are willing to offer over time.

Identity authentication and transaction monitoring processes are designed for two main purposes: (1) to meet legal obligations particularly relating to AML/CFT, and (2) to protect against losses from fraud. Historically, FIs have often managed anti-fraud and AML/CFT functions through separate teams located in different parts of their organizational structures, making collaboration difficult. Teams and information are also siloed by product lines or payment channels in some FIs.

While machine learning and other predictive models have been used for some fraud detection activities for several decades, categorical, rules-based models that flag transactions of a certain size or meeting other thresholds have historically been more common for AML/CFT. However, there are both efficacy and inclusion disadvantages to these traditional approaches, and practices are shifting. As discussed below and further in Section 6, these shifts could have both positive and negative effects on consumer access depending on implementation.

4.1 Legal frameworks

In the US, requirements for AML monitoring functions are set forth in the BSA. Anti-fraud processes are driven in part by the Fair Credit Reporting Act (FCRA), which requires FIs to monitor for identity theft,[93] as well as by general incentives to reduce losses for consumers and FIs under several other laws.

The BSA sets forth AML transaction monitoring requirements that largely concern payment transparency and transaction reporting. The BSA's Recordkeeping and Travel Rules (Travel Rule) generally require FIs to collect and retain information about the originator of a transaction of $3,000 or greater as well as to transmit that information to other FIs participating in the transfer.[94] The rules do not apply to various types of electronic fund transfers, including transactions made through ATMs, point of sale systems (PoS), or automated clearing house (ACH) transfers.[95]

In cases where the Travel Rule applies, the originator's FI must transmit the originator's name, address, and account number (if one exists), and the identity of the beneficiary's FI, the payment amount, and the payment date. The originator's FI may also optionally include the final recipient's address and their account number or other identifying information.[96] Intermediary FIs in the transaction must also transmit this information to the next FI in the payment chain until it reaches the final recipient. Non-banks are also generally required to verify the identity of the person placing the transmittal order or receiving the funds if they are not already established customers.[97]

AML requirements to report certain transactions to the federal government, such as through SARs[98] and Currency Transaction Reports (CTRs),[99] also sometimes specify customer identification and verification requirements. FIs file both SARs and CTRs to FinCEN through its e-filing system, where FinCEN analyzes them and makes them available to law enforcement and bank supervisory agencies.[100] SARs are required when a transaction is over $5,000 (or over $2,000 for MSBs) and any of the following are true: there is suspected money laundering, the transaction is out-of-pattern in some way,[101] the transaction serves no apparent legal or business purpose, or there is a suspicion of structuring to evade the stated reporting threshold.[102] They can also be filed in other circumstances where FIs suspect violation of a law or regulation. SARs include identifying information on the involved parties, the date of the incident, a reason code for why the SAR was filed, and a narrative description of the transaction. SARs do not require reporting of the institution and account holder that received outbound funds, though such information may be included in narrative fields.[103]

Additionally, FIs must file CTRs for transactions totaling $10,000 or more in a single business day, even without any suspicion of fraud or money laundering. CTRs contain similar information to SARs but additionally require the FI to reverify the originator's identity through a valid ID other than a bank signature card "that is normally acceptable as a means of identification when cashing checks for non-depositors (e.g., a driver's license or credit card)."[104]

More broadly, banks are also subject to the Customer Due Diligence Rule (CDD Rule), which stipulates that banks must "understand the nature and purpose of customer relationships and to develop customer risk profiles." The CDD Rule also requires banks to "conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information."[105] CDD requirements facilitate accurately flagging and reporting transactions for SAR and CTR requirements and providing accurate information for Travel Rule purposes.

For fraud, the Red Flags Rule in the FCRA requires financial institutions to have an Identity Theft Prevention Program. Among other requirements, this program must identify "red flags" of potential identity theft in day-to-day operations, including the monitoring of suspicious transactions, and define appropriate actions for when red flags are detected.[106] These requirements apply to both bank and non-bank FIs. FIs are also motivated to have rigorous anti-fraud programs because they absorb costs from dispute resolution and from fraudulent transactions that exceed liability limitations set for consumers under the Fair Credit Billing Act, the Electronic Fund Transfer Act (EFTA), and the Uniform Commercial Code depending on the payments channel and circumstances.[107]

BOX 9 EFFICACY OF ANTI-MONEY LAUNDERING EFFORTS

The existing AML regime is costly and extremely ineffective. While it is impossible to measure the exact extent of money laundering, estimates for money laundering and terrorist finance flows through the global banking system totaled $3.1 trillion in 2023 and range from 2 to 5 percent of global GDP annually.[108] Despite tens of billions spent on AML efforts each year,[109] only about 1 percent of laundered monies are recovered.[110]

Several factors contribute to these dynamics. One is the lack of a feedback loop between FIs and law enforcement, such that FIs rarely receive feedback about what SARs are useful for law enforcement. Government agencies' information sharing is often limited both by legal restrictions and by broader norms against sharing information about ongoing investigations for fear of leaks.[111] FIs are therefore unaware of whether law enforcement takes action as a result of their report unless agencies contact them for additional information. A 2017 survey of large banks by the Bank Policy Institute found that respondents received law enforcement inquiries on a median of only 4 percent of SARs filed, and average false positive rates for rules-based AML transaction monitoring systems are estimated to exceed 90 percent.[112] Legislation enacted in 2020 directs FinCEN to provide periodic summary feedback on SAR information that proved useful for law enforcement "to the extent practicable," but this has not yet been implemented.[113]

Another factor is the strong incentive to err on the side of over-reporting (sometimes called "defensive filing") to reduce risks that FIs will be deemed to have failed to satisfy regulatory compliance expectations, which increases filing volumes and costs over time. Although mistakenly flagging legitimate transactions as suspicious does have downsides—including increased compliance costs from follow up reviews, customer frustration about delayed or blocked transactions, and occasional concerns about liability[114]—the result is a system that tends to quantify and incentivize investments in reporting volume rather than reporting effectiveness. Even measuring the effectiveness of AML tools is challenging in this context.[115]

While money laundering is often addressed in isolation as white-collar crime, the failure of AML efforts has enabled and encouraged crime more broadly, including human trafficking and the distribution of child sexual abuse materials. In October 2024, federal regulators announced the largest AML penalty ever against a FI, imposing fines of more than $3 billion against TD Bank and capping its ability to grow after it pleaded guilty to willfully failing to implement and maintain an AML program that meets federal standards. Regulators faulted the bank for failure to detect evidence of human trafficking in payments as well as failing to file SARs on approximately $1.5 billion in suspicious transactions.[116]

BOX 10 FRAUD VERSUS SCAMS

As discussed in Section 2, both fraud and scams have escalated significantly since the pandemic.[117] While these terms are often used interchangeably in other contexts, the terminology has important distinctions in the financial services ecosystem. Fraud is generally used to refer to situations in which a failure in a bank's process for identity proofing allows a third-party fraudster to make unauthorized transactions from a customer's account, apply for credit with a stolen or synthetic identity, or otherwise intentionally misrepresent their identity to deceive a FI, although "first-party fraud" is used to describe situations in which FI customers themselves attempt to obtain funds or avoid liabilities by deceiving their FI.[118] In contrast, scams result in payments initiated in good faith by a consumer who has been deceived by a fraudulent third party. Examples of scams include when someone contacts an account holder with fake requests for an urgent payment that the account holder initiates without recognizing the deception.

Fraud and scams differ both as to defensive measures and liability. More robust verification and screening procedures are likely to stop fraudulent, unauthorized transactions by third parties and some types of first-party fraud but not scams where the account holder authorizes the transaction. Under rules implementing the EFTA, consumers' liability is limited for third-party fraud and other unauthorized transfers that are effectuated by debit or ACH channels if they are reported in a timely fashion, effectively requiring the FI to bear the loss if it cannot recover the money. However, EFTA rules do not apply to wire transfers or require reimbursement of scams,[119] though banks may try to help consumers recover funds where practicable, provide educational materials, or support other anti-scam initiatives for customers.

Several recent reports detail the need for national fraud and scam prevention strategies in the US and highlight the value of better data sharing and cooperation among FIs, telecommunications and social media companies, law enforcement, and other stakeholders.[120] The Aspen Institute's Financial Security Program is launching a national task force to coordinate and support fraud and scam prevention initiatives.[121]

4.2 Industry practices

FIs first authenticate a customer before the customer can initiate a transaction. For in-person transactions, for instance at a bank branch, authentication often involves presenting a valid government-issued ID. Authentication can also be accomplished with an ATM or debit card and a personal PIN, requiring that the consumer present their card to a reader.

For digital channels, customers typically use login credentials. These authentication channels are secured by back-end processes that check for signals of potential fraud. For instance, if a customer is authenticating from an unusual location or using an unrecognized device, FIs subject them to additional security measures such as two-factor authentication (2FA) or knowledge-based verification questions—often based on credit bureau data—to confirm their identity. However, expert interviews reveal these knowledge-based verification questions are highly ineffective.[122] Additional security measures may also include a "liveness test" where biometric facial recognition technology compares a short video the user takes of themself to their photo ID. If an individual fails to authenticate, they may have to reassert their identity by presenting an ID in person.

FIs' anti-fraud transaction monitoring efforts typically utilize behavioral profiles of individual customers or categories of customers. These profiles are built using various data points, including past transaction history, account usage patterns, and customer information collected at account opening (e.g., age and address). Once a baseline profile is established and the customer is authenticated, transactions are monitored in real time and receive a fraud risk score based on how they deviate from the customer's expected behavior. These profiling and scoring systems can involve both rules-based and machine learning models of varying complexity.

Like account opening, risk models are often used during transaction monitoring to assess the likelihood of fraud or illicit activity. The system either accepts, rejects, or flags a transaction for further review based on risk score thresholds the FI has previously set. Moderately risky transactions, especially by customers the FI's anti-fraud models struggle to evaluate, may be subject to additional scrutiny, such as manual review by a specialist or step-up verification processes such as requiring customers to use 2FA or verifying additional identity documents to complete the transaction.

For AML/CFT purposes, transaction monitoring processes typically examine longer transaction histories than anti-fraud models to identify out-of-pattern transactions, with increased scrutiny for larger transactions, especially for those above the SAR thresholds so that FIs can satisfy reporting requirements.[123] Many institutions rely primarily on rules-based AML/CFT systems that trigger further review when particular scenarios occur, while conducting extensive statistical analyses on a periodic basis to decide how to set and adjust particular thresholds and rules. However, use of machine learning and artificial intelligence tools is increasing in this context as discussed further in Section 6.2.[124]

In both contexts, monitoring and investigation are typically more rigorous for large transactions, as these are considered higher risk for potential illicit activities and lead to greater losses for the FI if the transaction is fraudulent and not prevented. Employing this risk-based approach to transaction monitoring helps to allocate FIs' compliance resources, focusing on the most suspicious activities while minimizing disruptions to customers. This risk-based process helps FIs protect their customers and maintain the integrity of the financial system more broadly.

One further complication in transaction monitoring has been the diversification of payments across channels that often provide less fraud-prevention infrastructure and in some cases faster processing times than other channels. While the infrastructure for debit and credit card transactions has been shaped by both regulation and network rules over the course of several decades, a growing range of companies are increasingly shifting to "pay by bank" channels such as ACH and so-called real time transactions.[125] Those channels do not have as much infrastructure for fraud monitoring, investigations, and dispute resolution among participants. Real-time channels also complicate monitoring and prevention activities, both because there is less time to detect, interrogate, and freeze potentially suspicious activity and because there is often no way to reverse transactions. As a result, upfront data collection and authentication become even more important in these contexts.[126]

Lastly, there is an important distinction between the capabilities of large and small FIs with regards to using technology to improve ID proofing and transaction monitoring. Most of the innovation in the transaction monitoring space is driven by third party vendors and by large banks that have access to significant pools of data and the scale to support technology teams that assess and test new technologies or new analytical approaches. This capacity is not shared by many smaller banks and credit unions, which have less access to data and analytical resources and rely heavily on core processors to provide transaction accounts and other core functions. While some core processors are moving to cloud based systems, providing artificial intelligence models to help their customers monitor across different transaction channels, and even experimenting with generative AI, working with legacy platforms can make it even more challenging for smaller depositories to keep up with evolving market trends.[127] The US Treasury Department described this issue as a "growing capability gap" in a 2024 report, noting that some stakeholders had questioned whether it would prompt customers to migrate to larger institutions. The Department plans to facilitate stakeholder conversations about core providers' adoption of AI monitoring models and to explore opportunities to collaborate in helping smaller institutions access AI capabilities.[128]

4.3 Financial inclusion concerns

Weaknesses in identity authentication protocols and transaction monitoring models that produce significant false positives or false negatives raise concerns for consumers' financial access and financial stability. Limited training data and reliance on static, rules-based systems, particularly in the AML context as described above, have been a continuing source of concern because they tend to produce large numbers of false positives that often trigger follow up investigations, payment delays or blocking, and disruption for both consumers and other counterparties in the payment transactions. Repeated AML flags or concerns that an account is receiving fraudulent transfers can prompt banks to close the accounts. At the same time, identity and related challenges in combating escalating fraud and scam activity puts consumers at greater risk of financial loss and other harms due to the failure to catch truly suspicious transactions.

False positives can affect consumers in multiple ways. One risk is that payments that they are trying to initiate get flagged as potentially fraudulent, leading to freezes or even account closures in extreme circumstances. Particularly in the e-commerce context, there is significant focus by merchants and vendors on the risks that these kinds of false positives will discourage consumers from completing individual purchase transactions.[129] However, there is very little data on the cumulative effects of false positives on consumers' finances and account access. Assorted sources estimate that the number of consumers who experience "false declines" on individual transactions or freezes on their credit card accounts due to concerns about fraud may be 15 to 25 percent,[130] but it is particularly difficult to evaluate how often transaction accounts are closed because the owner is suspected to be the victim of identity theft or other fraudulent activity.

False positives with regard to inbound deposits can potentially lead to freezes and account closures where banks are concerned that the consumer is receiving fraudulent proceeds. Statistics are extremely difficult to obtain, but consumer advocates and attorneys report that they have seen some instances where a single large anomalous deposit—even for items such as a tax refund or a lawsuit settlement—appears to have prompted an account closure.[131] The CFPB also ordered one bank to pay $160 million in connection with freezing or closing more than one million consumers' transaction accounts between 2011 and 2016 because it believed based largely on automated monitoring systems that the accounts had received a fraudulent transfer.[132] Several high profile cases of widespread account and benefit card freezes were also reported during the early days of the pandemic, leading in some cases to lawsuits and enforcement actions over the failure to respond quickly to legitimate consumers who could not access their funds.[133]

In the AML context, data on the rate at which financial institutions "de-risk" by closing accounts that have been subject to repeated suspicious activity is also extremely difficult to find.[134] In 2017, a Bank Policy Institute survey of a dozen large institutions found that a median of 28 percent of SARs filings resulted in terminated account relationships because repeat filings had been triggered over time.[135] Government Accountability Office surveys prior to the pandemic suggest that banks along the southwestern border of the US closed significant numbers of accounts and in some cases branches where SARs filings were highest.[136]

BOX 11 CHALLENGES WITH TRANSACTION ACCOUNT CLOSURES

Where transaction accounts are closed due to concerns about fraud or AML activity, consumers often scramble to determine what has gone wrong, appeal the decision, cover upcoming payments while they work to obtain their account funds, and open accounts at other institutions.

Federal fair lending laws require the provision of "adverse action" notices providing the specific, principal reason(s) why a lender has rejected a credit application or shut down an existing account, as well as information about third party information sources that the lender relied upon to make the decision.[137] Except where financial services providers rely on information in consumer reports,[138] other federal consumer laws do not contain such explicit disclosure provisions with regard to denials or terminations of other types of retail financial products and services although some consumer advocates argue that consumers' inability to complete transactions due to frozen or closed accounts should be treated as an "error" under the Electronic Fund Transfer Act, triggering investigation and explanation obligations by FIs.[139] Transaction account agreements generally give FIs the ability to close the accounts at any time for any reason without advance notice to consumers, although some states' laws may require some FIs to provide advance notice.[140]

FIs' explanations for account closures are also often limited. Federal laws prohibit providing any information that would reveal that SAR has been filed, though they do not prohibit the disclosure of underlying facts, transactions, or documents.[141] However, FI staff say they often feel constrained both by the legal restrictions and by more general concerns that providing detailed explanations could potentially give bad actors information that they could use to their advantage.[142] Consumers can reach out to FIs' customer service teams or to regulatory agencies, such as the Consumer Financial Protection Bureau or other state or federal regulators, where they believe a mistake has been made but it is unclear how often such complaints or appeals succeed.[143]

Where transaction accounts are closed, positive balances must be returned to the consumer, but timelines vary under different states' laws and consumer advocates report that delays are frequent.[144] The Consumer Financial Protection Bureau took action against several companies over delays unfreezing accounts and/or returning funds in the course of responding to widespread fraud suspicions during the pandemic.[145]

Situations in which consumers are reported as having been involved in suspected fraud to specialized consumer reporting agencies such as ChexSystems or Early Warning Services can also be challenging, since more than 80 percent of banks use such agencies' reports and are generally extremely reluctant to open accounts for consumers with such notations in their file.[146] Both entities are obligated under federal law to provide free copies of their reports to consumers under certain circumstances and to respond to disputes filed by consumers who believe that information in their file is incorrect.[147] However, advocates report that consumer awareness of the two companies is low, processes are difficult to navigate, and that successful challenges are rare in practice.[148] Information generally remains on both companies' systems for five years unless it is removed in connection with a dispute.[149]

As fraud reports and SARs filings have surged since the pandemic, annual consumer complaints to the CFPB about transaction account closures have doubled but remain relatively modest at about 3,000 complaints in 2023.[150] As noted in Section 2, news reports suggest that account closures are rising in part because financial institutions are relying more heavily on automated processes as SAR filing volumes have increased rapidly since the pandemic. Bank stakeholders in interviews and published columns have emphasized that they take account terminations very seriously, however, and that they do not leave such actions to automated decision making.[151] Some stakeholders suggested that account closures may be more likely at large banks for a variety of reasons, including the fact that they are often experiencing more fraudulent activity and that individual employees may be less familiar with individual customers than in community institutions. Some also noted that there can be more generalized economic factors that prompt banks to close very small dollar, inactive accounts, separate from concerns about suspicious activity.

Available statistics do not address customer demographics for transaction blocking or account closure, but there is a risk of disproportionate effects on LMI consumers and minorities from false positives and related processes. For instance, to the extent that transaction monitoring models associate the use of a prepaid phone or frequent address changes with fraud risk, all of these inputs are also correlated with income. Where transactions are escalated to manual review, there can be a natural bias toward blocking them because letting them proceed would require additional monitoring costs as well as raising risk levels. Interviews with stakeholders also suggest that it is not uncommon for those who lose access to identifying documents over time—particularly for housing insecure individuals—to lose access to their accounts as well because they cannot pass step-up verification procedures on flagged transactions.

At the same time, false negatives for fraud and scams (i.e., when a fraudulent transaction is not prevented) can also have a disproportionate impact on vulnerable populations, degrading their financial stability and ability to access financial services where they suffer losses or their credit histories are damaged. Various surveys and analyses of fraud losses by government agencies and consumer advocacy groups have found that Black and in some cases Hispanic consumers are more likely to have experienced various types of financial fraud and scams, and identity theft likely affects women and Black individuals disproportionately as well.[152] Research also suggests that consumers who are under substantial financial strains are more likely to be the victim of scams.[153] Although evidence regarding fraud victimization and age suggests that various age groups may experience different types of fraud more frequently, elderly consumers' fraud losses tend to be larger and may have particularly severe financial and emotional effects due to limited incomes and other factors.[154]

5. IDENTITY AUTHENTICATION AND MONITORING OF CROSS-BORDER PAYMENTS

Cross-border transaction monitoring involves largely the same types of inclusion risks as domestic monitoring: the blockage of individual transactions, mistaken closures of legitimate accounts, and failures in blocking illegitimate transactions depleting household resources. However, cross-border transactions are typically held to additional scrutiny in monitoring for AML/CFT. Furthermore, many FIs refuse to provide banking services to institutions in countries they deem to have high illicit finance or corruption risk—often based on government reports identifying particular countries as having "insufficient" controls, many of which are emerging economies with substantial low- to moderate-income populations—rather than institute additional monitoring or other safeguards for risk management.

Cross-border transactions also present operational challenges for FIs, including managing legal and regulatory asymmetries between the domestic FI and its international counterparty, such as varying privacy laws and reporting requirements across jurisdictions. However, the Financial Action Task Force (FATF), an intergovernmental body, provides some guidance on how countries can implement consistent best practices.

The net effect of these additional frictions can have substantial impacts on access to financial services, and migrants in the US often find it challenging to send remittances to relatives at home.

5.1 Legal frameworks

Legal requirements for the monitoring of international, cross-border payments are largely the same as those for domestic payments, including the SAR and CTR reporting requirements, the Travel Rule, CDD requirements, and the Red Flags Rule. Yet cross-border transactions present additional challenges, including legal and regulatory asymmetries between the domestic FI and its international counterparty—even if both the domestic customer and the international customer use the same multinational FI—such as varying privacy laws and reporting requirements across jurisdictions.

Cross-border transactions also magnify the importance of compliance with US sanctions administered by OFAC.[155] OFAC requirements apply to domestic FIs and to US banks' international banking facilities, as well as to their foreign branches and subsidiaries.[156] Foreign FIs also generally crosscheck customers with OFAC lists as part of their KYC processes, due to OFAC's expansive jurisdiction and the US's deep integration into the international financial system.[157]

The Financial Action Task Force provides some level of consistency in AML/CFT regulations across countries as well, although specific practices still differ across countries. The FATF issues standards and recommendations to combat money laundering and terrorist financing. The FATF maintains 40 recommendations for AML/CFT that range from the criminalization of money laundering to best practices for payment transparency.[158] The FATF recommendations provide the global standard for AML/CFT practices, with 38 member states, including all G20 countries, and over 200 jurisdictions committed to the recommendations through FATF membership or membership in partnered regional bodies.[159]

In the US, the BSA and its associated rules and regulations implement most of the FATF recommendations, with the FATF finding the US non-compliant with only 3 recommendations.[160] There are key differences between FATF and BSA requirements, however. For instance, the BSA Travel Rule—which requires additional information about the originator to be sent along with payments—implements much of FATF Recommendation 16 (R.16) but exempts transactions under $3,000 instead of R.16's threshold requirement of $1,000 or less. FATF recently proposed revisions to R.16 in an effort to increase transparency and better align requirements with payment messaging standards, as discussed further in Appendix A, but the changes would not affect the basic threshold.

The FATF monitors compliance through periodic country assessments and holds non-compliant countries to account by naming them a "Jurisdiction under Increased Monitoring" (on the "gray list") or a High Risk Jurisdiction (on the "black list").[161] Gray list countries have committed to quickly reach FATF compliance, and the FATF does not call for enhanced due diligence when FIs transact with them. On the other hand, the FATF *does* recommend enhanced due diligence when transacting with black list countries, and it can recommend other countermeasures that could include severely limiting business relationships with the country.[162] In practice, black list countries are largely cut off from the international financial system, and FIs limit their transaction exposure to gray list countries. This creates a strong incentive for countries to adhere to FATF recommendations even though the FATF has no direct powers of enforcement.

5.2 Industry practices

While the technical processes for customer authentication and transaction monitoring in cross-border payments are largely the same as those for domestic payments, legal and regulatory asymmetries between the domestic FI and its international counterparty add further complexity.

International transactions generally present higher money laundering and fraud risk, and FIs therefore subject them to additional scrutiny and often place lower limits on international deposits, ATM withdrawals, and cross-border transactions. FIs also typically tier AML and fraud risk based on the country of the international counterparty and may consider transactions with individuals in some countries too risky to complete. These high-risk countries may be on the FATF gray or black lists or be subject to US sanctions. Conversely, domestic FIs transacting with FIs in FATF-compliant countries have some assurance that their foreign counterparty conducted appropriate KYC procedures. These include periodic OFAC screening of existing customers, OFAC screening at account opening, and that the international counterparty can relay commonly required information with transactions.

However, differential legal requirements still pose challenges. For instance, data localization laws that require customer data to remain in its country of origin can make it difficult for FIs to detect fraudulent transactions across borders, even if the same multinational FI is on both sides of a transaction.[163] More generally, navigating different AML/CFT regimes across countries requires a depth of technical and legal expertise that is expensive and challenging for smaller institutions to achieve.

OFAC compliance is also particularly important in cross-border transactions. FIs that engage in more cross-border transactions or have more foreign customers typically conduct OFAC screenings of their existing customers more frequently. FIs also often run OFAC checks on the originator and recipient of an international transaction before executing it. For example, Nacha—the governing body of the ACH network—requires both OFAC screenings and the inclusion of Travel Rule information with international ACH transactions.[164]

Identifying the foreign recipient or originator of a transaction can be challenging, particularly for low-value transactions below FATF R.16 or Travel Rule thresholds and for transactions with foreign FIs that lack robust KYC processes. This challenge is exacerbated when transactions go through or between multiple intermediaries to ultimately enable receipt of funds through the intended recipient's bank—and often through the recipient's mobile payments, fintech and/or digital asset services provider. International end-to-end payments providers that maintain robust onboarding regimes and update customers' risk profiles can overcome this information asymmetry, however.[165]

5.3 Financial inclusion concerns

Cross-border payments include both business transfers and consumer remittances, which often display significant differences both in terms of the size of the transactions and in the ability to clearly identify the sending and recipient entities.

De-risking, when FIs terminate or restrict relationships with customers or categories of customers to avoid risk rather than assessing and managing it on an ongoing basis, is a major driver of exclusion in remittances and cross-border payments.[166] FIs often refuse to do business with MSBs or charitable organizations that operate in areas with high illicit finance risk, including many low- and middle-income countries. Similarly, US correspondent banks often refuse to do business with foreign FIs in high-risk areas.[167] Low- and middle-income countries are especially vulnerable to de-risking because perceived costs and challenges of AML/CFT compliance often outweigh expected revenue from serving the area.[168] Even when individuals have access to most financial services in the US, de-risking can leave them unable to send remittances to affected areas abroad. Some consumers in the US have also complained that their accounts have been closed not because of specific individual transactions but due to broader perceived OFAC risk due to their national origin.[169]

Some stakeholders have also raised concerns that FATF's recently proposed revisions to R.16 will make it difficult for FIs to serve lower-income consumers internationally. See Appendix A for more discussion.

6. EMERGING DATA AND TECHNOLOGY SOLUTIONS

As data and technology options continue to evolve, they are attracting heightened attention from financial institutions, regulators, and other stakeholders both as a means of making current processes more effective, efficient, and inclusive and defending against the evolving use of data and technology by fraudsters and other bad actors.

While some initiatives involve multiple components, at least three overlapping trends are emerging:

- Expansion of the data sources used in identity proofing, including both the companies supplying the data and the type of data being used, particularly in the context of authenticating customers while processing individual transactions;
- Adoption of more sophisticated analytical tools, as large FIs and vendors are increasingly developing and deploying more complex techniques and forms of artificial intelligence, particularly in response to concerns about deepfakes and other uses of AI to bypass existing systems; and
- Initiatives and tools to improve data sharing infrastructure, ranging from cross-industry platforms to use of privacy enhancing technologies such as encryption, federated learning, and other mechanisms to minimize the collection of data in a single location where it might be subject to attack or disclosure.

Stakeholders are still working to assess the effectiveness of various data sources, analytical techniques, and privacy-enhancing strategies. These innovations also raise important questions about whether and how federal consumer financial laws, model risk management guidance, and responsible AI principles should be adapted and applied in the context of combating illicit activity that itself can present customer protection concerns. Thus, as financial institutions rush to defend against fraud, it is also important to consider the impact of these innovations on general policy goals such as financial inclusion, fairness, privacy, and data security. While many of these initiatives hold promise for increasing inclusion and privacy protection, it is critical to consider the risk of unintended consequences on financially vulnerable populations.

BOX 12 WORK TOWARD COMPREHENSIVE US DATA PROTECTION FRAMEWORKS

US data privacy and protection laws have tended to focus on specific sectors with particular sensitivities, such as financial services and health care. Even in those sectors, however, legislative and regulatory action has not always kept up with market and technology evolution. For instance, the financial services sector has seen tremendous change since the Gramm-Leach-Bliley Act of 1999 adopted a relatively uniform baseline for data privacy and security of consumers' financial information, and regulations to implement laws adopted in 2010 that address customer-permissioned transfers of financial data were released in October 2024, as discussed further below.[170]

Interest in adopting a comprehensive US framework has increased in response to general trends toward digitalization, the European Union's adoption of the General Data Protection Regulation in 2016, and enactment of the California Consumer Privacy Act in 2018. In the identity context, such a law could be particularly important in shaping how both commercial entities and governments use, store, and protect consumer information.

However, discussions in Congress are complicated by committee structures that give different groups jurisdiction over different subsets of affected entities and by disagreements over whether a federal standard would permit private enforcement and act as a floor or ceiling on state initiatives. A bipartisan bill was reported out of committee to the House of Representatives in 2022,[171] but a successor bill was pulled back by House leadership hours before committee markup in June 2024 and had not been rescheduled as of the time of report publication.[172]

6.1 Expanding data sources

While initiatives to encourage FIs to accept a broader range of government IDs for identity proofing have moved slowly as discussed in Section 3, market practices are evolving with regard to what kinds of supplemental information FIs rely upon both at account opening and when authenticating identity during downstream transactions.

As large data breaches have become more common, basic biographic information and answers to common knowledge-based verification questions are increasingly available for sale on the dark web. In response, FIs and credit bureaus are increasingly analyzing biographic information across a broader range of separate data sources and/or with vendors that screen applications for a broad range of different financial service providers. One vendor, for example, reviews more than one million account applications per day and detects fraud by flagging when the same biographic data elements are used across applications at multiple FIs.

While biometrics also offer promise in some settings, fraudsters are already using sophisticated AI tools to create deepfakes of victims' voices and faces, and interviews with stakeholders reveal concerns that, just like biographic information, fingerprints and iris scans may be leaked in data breaches. With these concerns about basic biographic information and biometrics, FIs are beginning to look at a broader range of behavioral data and data from an individual's "digital footprint," such as an individual's activity across multiple companies, apps, and digital services.

Examples of this expanded range of data sources for identity verification and authentication can include:

- The consistency of association between an applicant's name, phone number, email, and other data elements across *multiple databases*, including information supplied by credit bureaus, data brokers, data aggregators, utilities, and phone carriers;
- An applicant's history with the same phone number, address, and email as reported by those same sources;
- Whether data elements are used on other reported stolen identities or recently used to open new (potentially fraudulent) accounts;

- Information collected from user devices, such as geolocation, the operating system and browser used, use of a VPN, use of a virtual camera, and keystroke timing;
- Whether a social media presence is consistent with biographic data;
- Liveness tests to see whether the biometrics of the presenter of identity information match biometric information provided (e.g., comparing a short video of the customer to a static reference image from a photo ID); and
- Other user activity in an online session—for instance if users update their passwords or addresses immediately prior to conducting large transactions.

Some data sources, such as keystroke timing and other patterns regarding physical use of a device, can be used absent any link to biographic data to try to distinguish humans from bots rather than to prove the identity of an individual. As FIs obtain permission to conduct verification activities and establish an account relationship with a customer, they can expand the range of data sources used and compare new sessions to prior interactions for authentication after initial account opening.

BOX 13 APPLICATION OF THE FCRA TO DATA FOR IDENTITY VERIFICATION AND FRAUD SCREENING

Congress enacted the Fair Credit Reporting Act in 1970 to regulate organizations that collect and supply information to unrelated companies and government agencies to determine consumers' eligibility for credit, insurance, employment, benefit programs, and various other goods and services by assessing the consumers' creditworthiness, capacity, and character.[173] To promote accuracy, privacy, security, and other policy goals, the law imposes obligations on these "consumer reporting agencies" (CRAs), as well as on parties that "furnish" them with information about individual consumers and/or purchase consumer reports from CRAs to make eligibility determinations and for various other purposes permitted under the law.[174]

Where information from a credit report about past credit or checking account history is used to reject an application for financial services, the FCRA requires that FIs provide a notice to consumers about the source and nature of the information.[175] However, many CRAs also provide data for identity verification and fraud screening that has historically been treated as falling outside the scope of the FCRA, although the information triggers privacy protections under the Gramm-Leach-Bliley Act.[176] For example, the Federal Trade Commission issued interpretations of the FCRA several decades ago concluding that basic biographic information such as name, address, date of birth, and SSN that appears at the top of CRAs' files (often called "credit header data") does not itself constitute a consumer report under the FCRA. CRAs often use header data alone or in combination with other information for other products and services relating to identity verification, fraud screening, and marketing, and include contract language prohibiting purchasers of those products and services from using the information for underwriting credit or performing other activities that are expressly regulated by the FCRA.[177]

Over time, another group of intermediaries called "data brokers" has sprung up to focus on data for activities that they argue fall entirely outside of the FCRA's scope, including but not limited to identity verification and fraud prevention. Like the CRAs, they typically include contract language prohibiting purchasers from using the information for activities that are expressly regulated by the FCRA. These companies have amassed information on millions of US consumers but are not widely known because they operate without consumer permission and do not follow FCRA disclosure requirements, and the Federal Trade Commission repeatedly urged Congress to adopt legislation to address privacy, accuracy, and data security concerns.[178]

With strong support from consumer advocates, the CFPB has recently signaled that it intends to change historical interpretations about the FCRA's boundaries through rulemakings that will classify data brokers as CRAs and credit header data as a consumer report.[179] More broadly, the CFPB also stated in a 2024 letter to the US Treasury Department that "because 'fraud screening' is used to assess credit-worthiness by determining who gets offered or approved for a financial product, firms that compile and provide such information are typically subject to the requirements of the Fair Credit Reporting Act."[180] Many FIs and other industry stakeholders are opposing changes to the treatment of credit header data, arguing that they reverse decades of precedent and could increase costs and uncertainty with regard to identity verification and fraud screening activities. Some stakeholders have also raised concerns that FCRA protections might be misused by bad actors, for instance through misuse of dispute processes or disclosures.[181]

Depending on how these data sources are utilized, they could have either inclusionary or exclusionary effects. Broadly, using a greater diversity of data can potentially help more consumers satisfy KYC requirements and reduce false positives in fraud or money laundering detection. Because the data may be derived from or stored in several different locations, it may be more difficult to falsify and more useful in facilitating the detection of falsifications and inconsistencies. For instance, a consistent association between an applicant's name and phone number across utilities, credit bureaus, phone carriers, and other services is difficult and costly for a fraudster to fake. Furthermore, using several of these data sources could potentially help FIs to verify the identity of customers who have less traditional forms of government ID, lack a credit bureau file, or have other factors that are associated with higher risk levels.

However, some data sources could also have exclusionary effects, for instance to the extent that systems focusing on address inconsistencies do not account for the fact that low-income individuals may tend to move more frequently. While identity proofing and fraud screening activities have not historically been subject to as much fair lending scrutiny as credit underwriting models,[182] the Consumer Financial Protection Bureau has stated in recent releases that the Equal Credit Opportunity Act (ECOA) applies in some circumstances to fraud screening activities, as well as the Fair Credit Reporting Act.[183] More broadly, the CFPB has also indicated that discrimination with regard to non-credit financial products and services may constitute an unfair act or practice, although that interpretation is being challenged in court.[184] Industry stakeholders report that fairness issues in fraud models are drawing increasing internal attention, although analytical frameworks that have been developed in the context of underwriting consumers for default risk may need to be adapted for activities focused on detecting whether the consumer is the victim of third-party fraud.[185]

BOX 14 USING OPEN BANKING INFRASTRUCTURE FOR IDENTITY PROOFING

So-called "open banking" infrastructure allows consumers to authorize the transfer of data that has accrued as they have obtained financial products or services from one FI to other FIs or general companies for the purpose of obtaining other goods and services. Thus, once a consumer has a transaction account, open banking transfers can potentially be used to help pre-populate information for KYC validation and expedite the process of obtaining other financial products and services, such as accessing payment apps or applying for credit. Indeed, one of the largest drivers of customer-permissioned data transfers in the United States is to help verify customers' accounts for payment platforms and the deposit of loan proceeds.[186] Detailed transaction account history can also provide important information to cross-check against other consumer data such as traditional credit report records.

Intermediaries called "data aggregators" serve as the hub of customer-permissioned data transfers as they move data between financial services providers or other companies at consumers' direction. Some of these companies have developed or acquired identity-specific services as part of their broader menu of offerings to financial services providers and are increasingly offering them to e-commerce, property management, and other non-financial companies as well.[187] Some are also involved in initiatives to facilitate information exchanges between FIs about fraudulent activity.

The Consumer Financial Protection Bureau issued final regulations in October 2024 to govern customer-permissioned transfers, including "basic account verification information," which is limited to name, address, email address, phone number, and a truncated account number or other account identifier in some circumstances, but excludes Social Security Numbers and information collected for the sole purpose of preventing fraud or money laundering.[188] Implementation of the rule is required for the largest banks by April 2026, although a legal challenge was filed on the day of release by banking trade organizations.[189] The CFPB's FCRA rulemaking discussed in Box 13 is also expected to classify data aggregators as consumer reporting agencies, despite arguments by some aggregators that they are different from traditional CRAs and data brokers because they act with customer permission in collecting and transferring data.[190]

6.2 Improving analytics

As discussed above, FIs often use a mix of rules-based and predictive models to validate identities and monitor for suspicious transactions and account behaviors. Anti-fraud modeling was one of the first contexts in which FIs began adopting machine learning models several decades ago,[191] and in recent years they have continued to adopt increasingly powerful predictive techniques in both account opening and transaction monitoring processes. AML processes are often still oriented toward rules-based thresholds and systems, but interest in machine learning and artificial intelligence systems is growing rapidly as transaction and data volumes increase.[192]

More advanced algorithms are appealing because they can map complex relationships to detect both fraud and illicit finance and can potentially further augment the value of using more and varied data, as discussed above. Particularly for detecting evolving practices and new vectors of attack, FIs view the combination of additional data sources and machine learning techniques as offering a chance to shift toward a more proactive posture in identifying evolving practices by bad actors. Stakeholders and researchers report that supervised machine learning algorithms such as neural networks, decision trees, and random forests can deliver significant performance increases over incumbent rules-based systems for detecting both fraud and illicit finance.[193] FIs are experimenting with a variety of approaches, including building scorecards to measure risk levels, mapping relationships between parties, and defining what "normal" transactions look like in order to train models to identify anomalies and deviations for closer reviews.[194] Some FIs and service providers are also beginning to use transformer models, which are typically used for generative AI applications, in transaction monitoring and other anti-fraud contexts.[195]

BOX 15 THE COMBINED EFFECTS OF ADVANCED ANALYTICS, BROADER DATA POOLS, AND PETs

In 2023, the BIS Innovation Hub published the results of "proof of concept" tests that compared the performance of models using more advanced analytical models such as logistic regression and various types of machine learning models as compared to traditional rules-based approaches for detecting money laundering in payments data. The tests also used some privacy enhancing technologies, as discussed further in Section 6.3. The models were built with different pools of synthetic data—institution-level, national, and cross-border—to further measure the value of training models with more holistic datasets.

The analyses confirmed that combining larger and particularly cross-border datasets with advanced analytics can substantially improve performance relative to traditional siloed data and rules-based models, even where PETs are applied to address privacy concerns. In general, the tests found that more sophisticated analytical models increased the detection of money laundering incidents by a factor of two to three over rules-based models, as well as reducing false positives by a similar magnitude. While logistic regression models performed relatively well on siloed/institutional level data, machine learning approaches were substantially stronger in analyzing national or cross-border datasets. Graph neural networks (GNNs) performed the best on each dataset in terms of accuracy and performed the best in terms of false positive reduction on the cross-border and national datasets. GNNs are machine learning models that analyze networks of interconnected nodes, which make them particularly powerful for transaction monitoring. This approach is promising for both AML and fraud detection, although decisions made with this approach are more difficult to explain because of the graphical nature of the data and analysis.[196]

While promising, the study emphasized the importance of additional testing with real-world data and noted a range of practical and policy issues that would need to be addressed to facilitate widespread adoption. The BIS announced a second phase of work in early 2024 that is designed to encourage real-world proofs of concept that can scale to eventual pilots, as well as beginning public-private dialogues around governance and a range of other policy issues.[197]

Several other academic studies also document substantial improvements from adopting more sophisticated predictive models to replace rules-based systems.[198]

BOX 16 ARTIFICIAL INTELLIGENCE AND GENERATIVE AI

The types of machine learning techniques that have been used historically in fraud and credit underwriting models are sometimes called "predictive AI." They use training data to develop models that predict a particular outcome, such as the likelihood that a transaction is fraudulent, when applied to additional data sets. More recently, the release of ChatGPT in November 2022 has sparked broad public interest in "generative AI" models that create new content (including text, images, audio, and video) that is similar to learned patterns in training data.

Bad actors can utilize generative AI to impersonate individuals or otherwise bypass anti-fraud and AML systems, for example by generating convincing "photographs" of fake IDs for presentation in online settings.[199] Voice cloning also uses generative AI to imitate a victim's voice and has raised questions about the future of voice authentication systems.[200] Financial system stakeholders are also exploring the potential defensive use of generative AI in identity verification and transaction monitoring applications, for instance to detect patterns in transaction data, generate synthetic data on which to train machine learning models, and to identify AI-generated content.[201]

Advanced analytics will also be an important layer of defense against new attack vectors from generative AI. For example, although generative AI that mimics victims' voices can bypass existing voice recognition systems, it is possible to apply additional analytics to detect these attacks by screening for unnaturally repeating tones or signs of the digital splicing of audio clips that are characteristic of AI-generated voice.[202] Liveness detection that requires users to record a video of themselves for verification or authentication is similarly vulnerable to AI imitations, yet a number of techniques to detect these imitations have emerged. These include the detection of virtual cameras and even analyzing miniscule changes in skin color to detect a user's heartbeat.[203] FIs are also using advanced analytics to verify the authenticity of physical IDs presented remotely through a user's camera, whether the fake ID is created with generative AI or more traditional methods.[204] As these analytics become more sophisticated, however, so do the capabilities of fraudsters and generative AI tools.

Overall, a more accurate assessment of a consumer's identity at account opening can potentially both combat identity theft and fraud and allow more legitimate consumers to access and use financial accounts. These analytics can also potentially reduce false positives in transaction monitoring, preventing consumers from having their legitimate transactions interrupted or losing access to their accounts altogether. However, ensuring that these technologies perform as expected and adapt to further evolution in the environment requires careful governance and oversight. As use of machine learning and AI techniques have spread to a broad range of non-fraud contexts in recent years, stakeholders are increasingly focused on the need to manage potential risks with regard to reliability, transparency, fairness, and other unintended consequences as predictive models, natural language processing, and other techniques become more complex. FinRegLab's previous work in the credit underwriting context has explored a number of these issues, as well as potential data science techniques for managing such concerns.[205] Although norms and requirements for underwriting models do not necessarily apply in the fraud context—for instance, expectations of transparency to consumers have historically been limited in dealing with potential illicit activity due to law enforcement concerns, as discussed in Section 4—it is unclear how and whether broader debates about responsible AI adoption may impact fraud and AML/CFT use cases. For example, explainability is still important for answering regulators' questions about how more complex models generate their predictions and what risks they are monitoring for.

BOX 17 RESPONSIBLE AI PRINCIPLES AND FEDERAL FINANCIAL REGULATORY EXPECTATIONS

As AI applications have been implemented across a growing range of sectors and use cases in recent years, stakeholders have begun debating the qualities or principles that support "responsible," "trustworthy," and "ethical" adoption and use. Reliability, fairness and inclusion, and transparency are among the most common qualities and principles cited across these various initiatives. For example, the European Union's recently adopted framework for regulating AI/ML builds on a 2019 European Commission formulation of seven key requirements for trustworthy AI: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability.[206] Other general frameworks for ethical/trustworthy AI are similar.[207]

In the United States, federal financial regulatory frameworks already incorporate elements of many of these principles, though the specifics vary to some extent by financial services provider and use case. For example:

- **General Risk Management and Model Governance:** To protect the safety and soundness of banks and the broader financial system, banks are expected to implement risk-based governance mechanisms for the development, deployment, and monitoring of models. These processes include analyzing whether models are relying on relationships in the data that are "conceptually sound" and assessing models' stability in changing data conditions. Both activities involve identifying features that are playing important roles in the model's operation.
- **Adverse Action Disclosures:** Federal laws require lenders to provide individualized disclosures to credit applicants of the "principal reasons" for rejecting an application and the "key factors" that are negatively affecting consumers' credit scores if the lender charges higher prices based on credit report information. As noted above, the FCRA also requires disclosures where information from consumer reports is used to take various adverse actions against consumers.
- **Fair Lending Compliance:** Federal fair lending laws generally prohibit both the use of race, gender, or other protected characteristics in underwriting models ("disparate treatment") and the use of facially neutral criteria that have a disproportionately adverse impact on protected groups unless the criteria further a legitimate business need that cannot reasonably be achieved through less impactful means ("disparate impact"). Traditional disparate impact compliance approaches often focus on testing whether omitting or modifying individual features that have been identified as driving disparities can improve fairness without substantial reductions in predictive accuracy.

For banks and nonbanks supervised by the CFPB, substantive compliance expectations apply where they outsource functions to outside vendors.[208] While adverse action and fair lending requirements apply to all lenders, in practice banks and larger non-bank lenders are supervised more closely for compliance.[209]

6.3 Improving data sharing infrastructures

A third set of interrelated initiatives and tools are focusing on data sharing infrastructures through a variety of strategies, ranging from use of vendors and new cross-industry platforms to technologies that can reduce the need to pool information in a single location while still improving identity proofing and transaction monitoring processes.

Vendors have long played an important role in identity proofing, fraud, and AML/CFT functions because their work with multiple individual financial institutions can provide broader insights than any one institution may be able to derive from analyzing its own data in isolation.[210] New entrants are working to build larger platforms that aggregate several data sources to provide a single point of integration for client FIs. Industry groups are also exploring the use of platforms for more direct data sharing for anti-fraud efforts and AML/CFT.[211] For example, the American Bankers Association is piloting an information exchange between member banks (particularly smaller institutions) to bolster anti-fraud and AML/CFT efforts,[212] and Capital One is engaged in a similar effort with payment providers Stripe and Ayden.[213] As discussed in Section 6.2, the Bank for International Settlements is also working to test "proofs of concept" regarding the potential impacts of combining advanced analytics with cross-border data for payments monitoring.

Data sharing improves fraud and illicit finance detection and may reduce false positives by allowing detection models to train on more data. Additionally, depending on how it is structured, data sharing has the potential to allow FIs access to granular historical data about customers who are new to the particular FIs but not new to the broader financial system. This kind of longitudinal data for new customers could allow FIs to create more precise risk profiles at account opening and likely improve anti-fraud and AML/CFT efforts considerably.

Section 314(b) of the Patriot Act is designed to encourage collaboration by providing FIs a safe harbor with liability protections when they voluntarily share data with one another to facilitate identifying and reporting activity that may be related to money laundering or terrorist financing activities.[214] However, there is no clear regulatory framework or widely used secure digital infrastructure in place to enable this data sharing.[215] Moreover, while regulators have signaled that the statutory provision is broad enough to facilitate data sharing with regard to fraud as a predicate activity that feeds into money laundering,[216] stakeholders report that getting FIs comfortable with sharing fraud-related information under the provision has delayed progress on some cross-industry initiatives. The US Treasury Department specifically highlighted the need for more information sharing on fraud topics in a 2024 report.[217] Although 314(b) registrations have been increasing particularly since the pandemic, including a coalition of very large banks, currently only about 8,000 institutions have given notice to federal regulators that they intend to participate in such a program.[218]

Consumer data security and privacy are also critical considerations in the context of data sharing initiatives, particularly given incongruent customer protection laws across different jurisdictions and the fact that larger accumulations of data containing substantial consumer information make more enticing targets for hackers. PETs—including forms of encryption, targeted differential privacy, federated machine learning, and techniques to generate synthetic data for use in training anti-fraud and AML models—hold promise for addressing these risks and operational challenges and for meeting privacy/confidentiality requirements applicable to governments and private actors, while retaining benefits from utilizing a wider ecosystem of data.[219] However, these techniques are at various stages of development, and broader testing would be helpful to facilitate potential implementation and policy initiatives.

Data sharing arrangements also pose technical challenges. Incorporating data from several FIs that use disparate data formats and operate in different environments into AML/CFT and anti-fraud systems is difficult. These challenges particularly impact data sharing for monitoring cross-border transactions, as data formats and the information included with different transactions differ from country to country. The adoption of standards for data formats and information included with transactions, such as ISO20022,[220] could help to ease these technical challenges.

Whether through a vendor or more direct collaboration, data sharing allows for more accurate detection of fraud and illicit finance and can reduce false positives that result in legitimate consumers having their transactions or account access interrupted or revoked permanently.[221] Data sharing is a promising avenue to improve identity proofing processes and financial inclusion, although privacy and security concerns must be managed carefully.

BOX 18 FEDERATED MACHINE LEARNING

Federated learning is a particularly promising PET in the AML and fraud context because it allows participants to train a machine learning model iteratively on different buckets of data, without having to share or move the training data directly.[222] Either alone or in combination with other PETs, this approach may improve anti-fraud and AML/CFT models by allowing institutions to benefit from a larger ecosystem of training data without creating large, consolidated pools of data that are likely to be targeted by hackers.

The BIS Innovation Hub's 2023 "proof of concept" tests suggested that federated models have significant promise.[223] While training machine learning models on a centralized set of cross-border data produced the strongest results overall, approaches that used federated machine learning to allow analysis of cross-border data without centralizing the data in one location were still more effective and resulted in fewer false positives than models trained on data from a single country. For example, one approach applied homomorphic encryption and local differential privacy to data aggregated at a national level and then trained a federated machine learning model using each country's aggregated data. The federated model detected about 70 percent of money laundering incidents, whereas a machine learning model trained only on national data detected about 60 percent and a traditional rules-based model detected about 25 percent. Both machine learning models reduced the number of false positives by roughly 75 percent relative to the rules-based model. However, these complex models were also less transparent and explainable than the rules-based model, and the study did not conduct an empirical analysis of the strength of the various privacy protections.

Stakeholder interviews suggest that federated learning may be particularly useful for monitoring international transactions, as data localization laws that require customer data to remain in its country of origin make it difficult to train models on data from several countries, even for extremely large FIs that operate in multiple jurisdictions. In addition, federated learning may be particularly useful for smaller institutions or vendors with limited training data of their own.

Vendors are offering federated learning models for AML screening and exploring their potential extension to fraud detection. However, widespread implementation potentially raises coordination challenges across institutions and countries, and data science research is continuing with regard to various potential concerns such as data leakages, accuracy tradeoffs, and computational burdens.[224]

BOX 19 WEB3 AND TOOLS FOR DATA EXCHANGE

As noted in Section 3, many stakeholders are also enthusiastic about the potential for decentralized "Web3" technologies, such as certain applications of tokenization and distributed ledger technology, to create "reusable KYC" that could facilitate information sharing between FIs while also giving consumers more control of their personal information.

For example, some organizations are using decentralized identifiers—which are unique identifiers that are tamper-proof, cryptographically secure, and authenticatable so that users can manage their identifying information across platforms—and privately-created "verifiable credentials" that operate similar to mDLs in providing cryptographically secure means of storing specific identity attributes or other compliance information.[225] Some are also using a form of cryptography called zero-knowledge proofs that essentially allow a yes/no query to be submitted to verify identifying information without disclosing it. For example, consumers could prove that they are 18 or older without divulging their birthdate.[226]

In the financial services context, advocates envision these technologies as being particularly useful to facilitate identity proofing in real time payments and other settings involving networks of FIs, particularly for smaller institutions with more limited resources and data for fraud screening. Once a network member verifies a customer through their KYC process and issues them a credential under this arrangement, consumers could supply the credential in connection with individual transactions or establish relationships directly with other members of the network using the credential rather than going through a second KYC process. These compliance-backed verifiable credentials can enable data sharing via explicit permissioning by the consumer and can be structured to avoid disclosing the underlying PII.

Various companies have been working to organize proof-of-concept initiatives in financial services both internationally and in the United States over the last several years,[227] but the pace of adoption is being affected by uncertainty with regard to regulatory acceptance and the legal and business relationships between participating FIs in addition to technological developments.[228]

7. POTENTIAL AREAS OF FOCUS

The convergence of new data and technology innovations and escalating fraud and scams costs is increasing attention to and investment in identity proofing and transaction monitoring. Although there appear to be substantial opportunities to improve the status quo for *both* financial institutions and their customers, there is also a substantial risk of unintended negative impacts on historically excluded and vulnerable populations. Achieving win-win outcomes is likely to depend on sustained engagement by a broad range of stakeholders to ensure consideration of the potential implications of new technologies and practices not only for combatting bad actors but also for impacts on financial inclusion and wellbeing and data privacy and security more broadly.

This section highlights the potential value of public empirical research, initiatives to reduce cost and efficiency frictions for FIs, and addressing emerging policy questions as a means of bridging knowledge gaps and expanding upon current projects while stakeholders continue to debate broader frameworks for data protection and digital identity.

7.1 Filling knowledge gaps

While larger FIs and vendors are evaluating the efficacy of new data sources and modeling innovations in the fraud context, those evaluations are limited to available data silos, may not consider the full range of inclusion and other customer protection implications, and are not accessible to the entire financial services ecosystem. Publicly available empirical research for benchmarking traditional systems and approaches is also limited. Better information on a range of topics could help policymakers and other stakeholders to prioritize the most promising initiatives and measure their outcomes:

1. **Mapping US identity gaps.** Factors that prevent consumers from securing government-issued IDs present a fundamental challenge to financial inclusion and lead to broader harms, including preventing individuals from receiving government benefits, finding housing and employment, and even from voting. They include situations in which original documentation was never issued, contains discrepancies, or has been lost, damaged, or expired, particularly where access to government offices to obtain or renew ID is limited. Available data suggest that these issues disproportionately impact LMI populations, people of color, and unhoused people, but the exact contours of these problems are less known to US policymakers than in the international context. Probing the relationship between lack of ID, lack of trust in banks, and concerns about lack of privacy among unbanked populations could also be helpful to better understand financial inclusion dynamics and the potential value of enhancing privacy protections in connection with identity proofing processes.

2. **Assessing potential downstream inclusion issues in transaction monitoring.** False positives that lead to the freezing or closure of legitimate accounts can have significant impacts on consumers' financial stability and access to financial services, but there is no reliable, consistent source for measuring the current scale of such issues in the US or the potential impacts of new anti-fraud initiatives.
3. **Evaluating the pros and cons of using non-traditional data sources for identity proofing.** FIs and other online platforms are increasingly leveraging consumers' digital footprints for transaction monitoring and verification of identity, for instance by analyzing when, where, and how an individual typically uses a service to determine if a login attempt is legitimate. Empirical research could be helpful to better understand how FIs and other online platforms are currently leveraging this information for authentication and transaction monitoring, to what extent it could potentially be useful for identity proofing at account opening, and whether it could reduce reliance on documentary ID. For example, research could help to inform policymakers and other stakeholders about the relative value of different types of data, as well as assessing the risks that particular types of information might create bias or privacy concerns. Research into the reliability of various types of documentation accepted by municipal ID programs could also be helpful to address FI concerns about broadening their identity verification processes beyond driver's licenses and state ID cards.
4. **Evaluating analytical tools and platforms for increasing data sharing while protecting privacy and security.** Privacy enhancing techniques such as federated learning offer significant potential for improving the accuracy of models while avoiding the centralization of sensitive data that can become a hacking target. Working with programs organized by the Bank for International Settlements or focusing on US-based initiatives to test these technologies with real-world data would help to answer critical questions about the risks of data leakage, accuracy tradeoffs, and computational burdens relative to other structures for data sharing.

Policymakers have a particularly critical role to play not only in financially supporting public research on such topics but in helping to manage data constraints that might otherwise make analysis impossible. Organizations such as the Bank for International Settlements and the United Kingdom's Financial Conduct Authority have developed synthetic datasets for some evaluations,[229] but real-world data are critical for measuring many baselines and the ultimate impacts of innovations. In some cases, government agencies may be the only organizations that can access and analyze the relevant data in light of legal restrictions, market and jurisdictional siloing, and broad-based concerns about protecting the confidentiality of law enforcement proceedings and highly sensitive personal information.

7.2 Reducing frictions through standardization and other on-the-ground initiatives

A second area of potential focus is on initiatives that could reduce frictions that may tend to discourage FIs from adopting more inclusive identity proofing programs and practices due to concerns such as cost and efficiency. These include initiatives encouraging standardization across less common forms of government-issued ID, facilitating interoperability and the adoption of standards in state mobile driver's license programs, and addressing frictions in SSN authentication and use of ITINs.

1. **Supporting standardization of government-issued identification.** Policymakers at both the state and the federal level could help to reduce FIs' concerns about accepting less common forms of government-issued IDs by working to align and standardize requirements for ID issuance, embedded security elements, and the form factor design of various government-issued documentation. Exploring the use of open source software packages in physical ID readers so that they can be more easily updated as form factors and security features evolve could also be beneficial to reduce the time and effort needed to adjust to changes in the market.

2. **Expanding upon current mobile driver's license initiatives.** Nearly 30 states are currently issuing or preparing to issue mDLs, which can offer more security for online transactions and facilitate renewals and replacements of expired, lost, damaged, or stolen physical IDs. Current initiatives to promote interoperability standards for online use cases and technical builds in the financial services context are important baseline steps. The extent to which federal financial services regulators engage with the NIST mDL implementation for financial accounts could be particularly critical in giving FIs confidence about how to treat mDLs in their customer identification processes.[230] More broadly, policymakers and other stakeholders can promote the efficient and inclusive expansion of mDL systems through supporting research and harmonization initiatives, considering options for consumers with limited identification documentation or digital access, and facilitating market practices and use cases that will help to scale adoption by both consumers and companies.

3. **Reducing SSN and ITIN frictions.** Potential improvements to the issuance of ITINs to facilitate more efficient and consistent issuance processes could include the adoption of modernized equipment to reduce document verification time and increasing the affordability of Certifying Acceptance Agents. These measures would reduce the need for applicants to mail in their IDs and be without their documentation for extended periods. Additionally, improving credit reporting procedures for ITIN holders would help to ensure that they do not lose credit or other financial histories in the event that they later obtain SSNs. Credit reporting agencies and other stakeholders could make these improvements in coordination with the Social Security Administration to ensure that the credit files of those with newly issued SSNs include the financial history associated with each individual's older ITIN.

7.3 Emerging policy questions

In addition to the need to fill knowledge gaps and reduce implementation frictions, stakeholders are also facing a range of emerging policy questions regarding the potential for data and analytical innovations to address the surge in fraud and scams and longstanding inclusion challenges. These include:

1. Whether and how to reduce current restrictions on and disincentives for financial system stakeholders to engage in data sharing in light of the increase in fraud and scams, and the efficacy of PETs and decentralized ID forms to address privacy and confidentiality concerns while improving the accuracy of identity proofing and transaction monitoring processes.

2. How to manage collective action challenges, particularly in international settings, to deploy federated machine learning models or other digital identification infrastructure across multiple institutions and jurisdictions.

3. Whether and how application of other general tenets of consumer protection, model risk management, and responsible AI use should be adapted for the fraud and AML/CFT context in light of current challenges and constraints, and the efficacy of various data science techniques in meeting regulators' expectations with regard to efficacy, explainability, fairness, or other concerns.
4. Whether and how to strengthen positive incentives to encourage FIs to invest in more inclusive identity proofing practices for populations that may be relatively unprofitable to serve, for instance by providing credit under the Community Reinvestment Act.
5. How to manage gaps in data access and technical resources among smaller banks, which are often heavily dependent on their core processors in modernizing their processes and tools. Adoption of innovative approaches may be particularly challenging for smaller FIs that lack the resources to build internal capabilities, integrate and manage relationships with third party providers and data sources, and manage more complex regulatory compliance. Yet if they cannot keep up with market developments and best practices, both the institutions and their customers could face greater risk of potential losses from bad actor activity and of missing out on market developments that could potentially improve financial inclusion.
6. The need for additional strategies for combating scams in addition to fraud, including the efficacy of consumer education initiatives, coordination with other sectors such as social media and telecommunications providers, potential revisions to legal frameworks, and other approaches.
7. What balance to strike with regard to security, convenience, and privacy in the context of faster payments. While both market actors and policymakers have been working to create frictionless payments experiences through various real time initiatives, such systems create an inherent tradeoff between privacy and security: For faster payments to be frictionless and secure, a great deal of personal data must be tracked and shared to ensure the integrity of the transactions. These tensions are causing some jurisdictions to rethink their approaches. For instance, in the United Kingdom, regulators have proposed revising faster payments systems to allow banks to delay transmission for up to four days to investigate where there is a suspicion of fraud.[231]
8. Whether risk-tiering of accounts could provide a viable inclusion strategy, either in its own right or as a supplemental safeguard when testing less traditional data sources or other approaches to increase financial inclusion.

In addition to these emerging questions, stakeholders are continuing to debate longer-term structural issues such as the contours of a comprehensive US data protection scheme and a more ambitious and comprehensive framework for digitally-based identity systems beyond mDL implementation. While these topics have attracted significant attention over the last several years and would provide critical context for anti-fraud and -scam initiatives, they have been substantially complicated by factors such as congressional committee structures, federal/state politics, political tensions over immigration, and network and competitive dynamics.

Given that these larger structural initiatives are still nascent, it is particularly important to involve a full spectrum of stakeholders in focusing on the potential implications of anti-fraud and scams initiatives and new developments in data and technology for identity proofing, including not only front-line FIs and technology companies but also advocates, academics, and policymakers. While FIs, vendors, and other technologists are strongly motivated to reduce losses, they are also motivated by commercial interests in securing market position and may be more attuned to some consumer impacts than other stakeholders. Ensuring that the full spectrum of consumer interests are considered and balanced in these initiatives—particularly for historically underserved communities and vulnerable populations—will require sustained engagement from a diverse spectrum of stakeholders.

Engagement from regulators and policymakers through tech sprints, innovation hubs, supervised market tests, and other platforms for dialogue could be instrumental in helping to identify, understand, and manage both the risks and opportunities of this particular moment. Increasing losses due to fraud and scams and recent headlines about the potential risks of generative AI deepfakes have injected urgency into discussions, but given the complexity of systems as described above, a narrow law enforcement approach could miss other important consumer protection, inclusion, and financial stability implications.

8. CONCLUSION

Identity proofing and transaction monitoring activities can have substantial impacts on consumers' financial inclusion and stability. Millions of Americans and people worldwide have gaps in their identity documentation that make it difficult for them to satisfy account opening requirements. At the same time, with significant data breaches and jumps in fraud rates, FIs are fighting to keep up with increasingly sophisticated fake physical IDs, synthetic identity fraud, AI deepfakes, and more. FIs are therefore shifting to more diverse data sources, more advanced analytical techniques, and new data sharing initiatives in order to mitigate these risks.

As these shifts occur, however, it is critical to consider their implications for financial inclusion, consumer protection, and other broader policy objectives. These innovations could have unintended negative consequences for vulnerable and historically underserved consumers, but they could also create opportunities for advancing financial inclusion and consumer privacy while better protecting FIs and consumers from bad actors. Sustained engagement by policymakers, industry, advocacy, and research stakeholders is needed to ensure that these new data and technology initiatives are structured in ways that help to close existing identity gaps, build long-term digital infrastructure, and reduce the risk of substantial unintended negative impacts on consumers and smaller institutions.

In particular, there is a need for additional empirical tests and research to analyze data and technology solutions for identity proofing and transaction monitoring, initiatives for reducing cost and efficiency frictions, and dialogue between stakeholders on emerging policy issues. FinRegLab is continuing to assess potential future workstreams on these topics. With the adage to "never let a crisis go to waste," this is a critical time for stakeholders to take a more holistic look at how identity affects financial inclusion, privacy, security, and user experience and to identify targeted improvements that can build momentum toward long-term infrastructure, such as data privacy frameworks and digital identity systems.

APPENDIX A

Proposed Revision to FATF R.16

Earlier in 2024, FATF began a public consultation on proposed revisions to R.16 (the FATF version of the Travel Rule), which concerns requirements for information about the originator and recipient relayed with certain payments, including wire transfers and transfers of cryptoassets.[232] The revisions aim to modernize the provision, expand it, increase transparency in connection with more types of payments, and align R.16 with the ISO 20022 payment messaging standard.[233] These revisions will impact billions of transactions annually and could have profound consequences for financial inclusion globally. In the US context, the implications for financial inclusion mainly center on international remittances.

Under R.16, qualifying cross-border payments (typically transactions of $1,000 or greater) must currently contain the originator's name and account number, as well as either their address, national identity number or other unique official identifier, customer identification number, or their place and date of birth. They must also include the beneficiary's name and account number. The proposal presents two options for revising this required information, which are outlined below in Table A.1.

TABLE A.1 REVISIONS TO REQUIRED INFORMATION TRANSMITTED WITH QUALIFYING CROSS-BORDER TRANSACTIONS

LENDER TYPE	INCLUDE *ALL* OF THE FOLLOWING:	INCLUDE *AT LEAST ONE* OF THE FOLLOWING
CURRENT RECOMMENDATION	» Originator's and beneficiary's name » Originator's and beneficiary's account number	» Originator's address » Originator's national identity number or unique official identifier » Originator's customer identity number » Originator's place and date of birth
"OPTION 1"	» Originator's and beneficiary's name » Originator's and beneficiary's account number » **Originator's and beneficiary's address (or country and town name when not available)**	» Originator's national identity number or unique official identifier » Originator's customer identity number » Originator's place and date of birth
"OPTION 2"	» Originator's and beneficiary's name » Originator's and beneficiary's account number » **Originator's and beneficiary's address (or country and town name when not available)**	» Originator's **and beneficiary's** national identity number or official identifier » Originator's **and beneficiary's** customer identity number » Originator's **and beneficiary's** place and date of birth

"Option 1" would mandate the inclusion of both the originator's and the beneficiary's address with all qualifying transactions.[234] However, the FATF permits country and town name to be used when address is not available, which should mitigate some exclusionary effects. Option 1 also continues to require inclusion of either the originator's national identity number, unique official identifier, customer identity number, or date and place of birth. Because these requirements typically apply to only transactions of $1,000 or more, a threshold that most international remittances sent from the US fall well below,[235] and place no more information requirements on the beneficiary, Option 1 may not have significant exclusionary effects in the US.

"Option 2" additionally mandates that qualifying cross-border payments also include either the beneficiary's national identity number, unique official identifier, customer identity number, or date and place of birth. Requiring the originator or the originating FI to acquire and transmit this personal identifying information about the beneficiary may have consumer privacy implications and may also present operational challenges for FIs. Furthermore, those with little documentation in low-income countries and countries subject to de-risking may find themselves excluded from both sending and receiving cross-border payments, as FIs in these countries tend to over-comply with AML/CFT requirements.[236] For example, an FI may require the customer's national identity number, customer identity number, and date and place of birth be included with payments when the FATF only requires one of these elements.[237]

R.16 currently exempts cross-border and domestic credit, debit, and prepaid card transactions for the purchase of goods or services from all of its information requirements, so long as the originator's card number accompanies the transaction.[238] However, the proposed revisions would narrow this exemption in various respects, narrowing the exemption to apply only to purchases from "merchants" and thus causing all credit, debit, and prepaid card transactions between individuals to be subject to the main requirements. The FATF's proposed "merchant" definition also does not include micro and small enterprises (MSEs) that use personal financial accounts or commingle personal and business finances. Another related concern involves the proposed requirement to use official identifiers for legal entities, as MSEs often do not use these identifiers and they can be expensive to obtain in many countries.[239] All card transfers with merchants would also be required to be accompanied by the name and location of the issuing and acquiring FIs in order to clarify with which FIs the originator of a card transaction has a relationship. The proposed revisions also include another "Option 2" that additionally removes R.16's exemption for withdrawals or purchases of cash or cash equivalents.[240] These revisions widen the applicability of the revised information requirements discussed above and may affect MSEs in low- and middle-income countries disproportionately.

These revisions could have profound effects, and whether they advance or harm financial inclusion in the aggregate depends on implementation and several contextual and interrelated factors. For instance, interviews with stakeholders suggest that the cost of updating card networks and other payment systems to comply with these revisions could impact the ability of FIs to serve low-income or historically excluded populations globally. These costs will be especially burdensome for smaller and community-based FIs that serve low-income customers and customers in rural areas. However, as these revisions align FATF requirements with the ISO20022 standard, compliance may lower costs in the long term by reducing manual processing and friction in translating disparate payment messaging standards.[241] Estimating the magnitude of these and other effects in the short and long term would require a thorough impact assessment, however, which the FATF has not undertaken.[242] More research on the consequences of this proposal for financial inclusion would be useful.

Endnotes

1 Demirguc-Kunt et al., "The Global Findex Database 2021."

2 Rothschild, Novey, and Hanmer, "Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge."

3 For a discussion of the impact of the lack of a trustworthy digital ID, see Better Identity Coalition, "Better Identity in America: A Blueprint for State Policymakers."

4 See, e.g., Bernard and Lieber, "Banks Are Closing Customer Accounts, With Little Explanation"; Lieber and Bernard, "Why Banks Are Suddenly Closing Down Customer Accounts"; Crossman, "Rushed Anti-Money-Laundering Calls Backfire. Can AI Help?"

5 The Better Identity Coalition uses the term "identity gaps" to discuss differences between various government-issued physical credentials in the United States and the lack of any digital counterparts that would allow people to use them in online environments. The Better Identity Coalition, "Better Identity in America: A Blueprint for Policymakers." This paper uses the term broadly to refer to problems in existing identity infrastructures that make it difficult for individuals to prove that they are who they say they are in both physical and online environments. Although this report focuses primarily on identity gaps for individual consumers, processes for verifying businesses and their ownership can be complicated for both entrepreneurs and financial institutions. New laws also require businesses to register directly with FinCen regarding their "beneficial ownership," subject to significant penalties. See, e.g., White et al., "Digital Identification: A Key to Inclusive Growth"; Moody's, "From KYC to KYB: The Key Differences and Best Practices"; Shepherd, Koff, and Schiffer, "Looming Reporting Deadline Under the Corporate Transparency Act."

6 Johnson and Dausin, "What to Know About the National Public Data Breach—Is It Worthy of the Hype?"; "Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High"; Morris, "The Number of Data Breach Victims Is up 490% in the First Half of 2024."

7 See Box 1.

8 Demirguc-Kunt et al., "The Global Findex Database 2021," 1–3, 35–36; The World Bank Group, "Volume 1: Global ID Coverage Estimates."

9 The World Bank Group, "ID4D and G2Px 2022 Annual Report."

10 "2021 FDIC National Survey of Unbanked and Underbanked Households," custom table generator.

11 Rothschild, Novey, and Hanmer, "Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge."

12 Movement Advancement Project, "The ID Divide: How Barriers to ID Impact Different Communities and Affect Us All"; Fines and Fees Justice Center, "Free to Drive: End Driver's License Suspensions for Unpaid Fines and Fees"; Rothschild, Novey, and Hanmer, "Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge" and additional analyses provided by the authors; Lindauer, "'Please Stop Telling Her to Leave.'"

13 "Identity-Related Suspicious Activity: 2021 Threats and Trends"; Gacki, "Prepared Remarks for the Identity Project Colloquium in Washington, DC"; "Financial Crimes Enforcement Network (FinCEN) Year in Review for FY 2023."

14 Estimates based on surveys and other sources vary from about 3 percent to 34 percent, with rates generally higher where the losses were more severe. Some evidence suggests that there are also differences in reporting among different demographic groups, so that people of color may be underrepresented in government statistics. Reporting rates to FIs tend to be substantially higher—often above 75 percent depending on the source and type of fraud—but some sources also find demographic disparities. The Federal Trade Commission, "Protecting Older Consumers 2022-2023"; Anderson, "To Whom Do Victims of Mass-Market Consumer Fraud Complain?"; DeLiema, Mottola, and Deevy, "Findings from a Pilot Study to Measure Financial Fraud in the United States"; Cruz, "52 Million Americans Experienced Credit Card Fraud Last Year"; Abraham et al., "The State of Scams in the United States of America"; Wei et al., "Serving Communities of Color," 41–16; AARP Research, "The Fraud Crisis in America: How Adult Consumers Feel, What They Know, and Their Actions That Pose Risks."

15 Federal Trade Commission, "Fraud Reports."

16 Nasdaq Verafin, "Global Financial Crime Report: Insights at the Intersection of Financial Crime Data & Real Survivor Rates."

17 Abraham et al., "The State of Scams in the United States of America."

18 Financial Crimes Enforcement Network, "SAR Stats."

19 Synthetic identity fraud occurs when a fraudster combines a victim's real information, such as their SSN, with invented information to create a fake identity. The fraudster then uses this identity to commit financial crimes.

20 Magramo, "Gangs Netting up to $3 Trillion a Year as Southeast Asia Human Trafficking Becomes a Global Crisis, Interpol Says"; Dilanian, Ramgopal, and Atkins, "'Easy Money': How International Scam Artists Pulled off an Epic Theft of Covid Benefits"; "Press Release: Justice Department Announces Results of Nationwide COVID-19 Fraud Enforcement Action"; "TransUnion Analysis Finds Synthetic Identity Fraud Growing to Record Levels"; Timoney, "Why Is Check Fraud Suddenly Rampant?"; McDonald, "Check Fraud Is Up Nearly 400% and FinCEN Points to Banks."

21 See Section 4.2 for a discussion of real-time payment channels. Horan, "Real-Time Payments Fraud Is Growing - Here's How to Prevent It"; PYMNTS, "Digital Wallets Exhibit Highest Increase in Fraud Among All Payment Methods"; FRB Services, "Fraud and Instant Payments: The Basics."

22 Interviews with banks and third party service providers.

23 Javelin Research, "Overcoming False Positive Declines in E-Commerce"; ClearSale, "State of Consumer Attitudes on Ecommerce, Fraud & CX 2021"; ClearSale, "Original Research Report 2024: Ecommerce False Declines & Consumer Behavior."; "2022 IBM Global Financial Fraud Impact Report."

24 Bernard and Lieber, "Banks Are Closing Customer Accounts, With Little Explanation"; Lieber and Bernard, "Why Banks Are Suddenly Closing Down Customer Accounts"; Crossman, "Rushed Anti-Money-Laundering Calls Backfire. Can AI Help?," (reporting about 3000 complaints in 2023, more than double the levels in 2020); Trew, "Closing the Book on Account Closures."

25 The FTC reported the median fraud loss in 2022 was $650. Federal Trade Commission, "Consumer Sentinel Network: Data Book 2022." Yet 37% of US adults in 2022 did not have enough savings for a $400 unexpected expense. Board of Governors of the Federal Reserve System, "Economic Well-Being of U.S. Households in 2022."

26 See, e.g., "Serving Communities of Color: A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color," 40; Medintz, "Black and Latino Consumers Are More Likely to Lose Money to Digital Scams, a Consumer Reports Study Finds"; DeLiema and Witt, "Profiling Consumers Who Reported Mass Marketing Scams: Demographic Characteristics and Emotional Sentiments Associated with Victimization."

27 "2023 Consumer Impact Report," 2023, 5; Identity Theft Resource Center, "Identity in Practice Report: Understanding Identity Crimes in Black Communities."

28 This paper discusses PETs in the context of mitigating the privacy and security impacts of expanded data usage, although emerging technologies like zero-knowledge proofs and decentralized identity systems may lead to more fundamental changes in how such information is managed.

29 The definitions for verification and authentication are based on NIST's Digital Identity Guidelines ("NIST SP 800-63 Digital Identity Guidelines") and FATF's Guidance on Digital Identity ("Guidance on Digital ID").

30 Financial institutions covered by the BSA include banks, money service businesses, businesses supervised by state banking authorities, broker-dealers, futures commission merchants, mutual funds, casinos & gaming businesses (31 CFR 1010.110(t)). Loan and finance companies that do not otherwise meet the definition of financial institution are subject to some AML requirements as well (31 CFR 1010.110(lll)).

31 31 CFR 1020.220(a)(2).

32 31 CFR 1020.220(a)(2)(ii).

33 MSBs are defined in 31 CFR 1010.100(ff). BSA regulations are somewhat more specific with regard to MSBs providing or selling prepaid access (e.g. a Visa Prepaid card), which are required to collect the same identifying information as banks, although the rules do not describe specific documentation or approaches. These verification requirements also apply to parties acting as sellers of prepaid access with regard to persons who obtain prepaid access to $10,000 or more in a single day. 31 CFR 1022.210(d)(1)(iv). However, MSBs that only participate in certain limited-scope prepaid programs are not subject to the more detailed verification requirements. For example, the definition of prepaid access excludes closed loop programs that are restricted to a maximum value of $2,000 per day and to programs that are restricted to a maximum of $1,000 per day, do not permit funds to be transferred internationally, and meet certain other restrictions. 31 CFR 1010.100(ff)(4)(iii)(A), (D).

34 Although this check is not an explicit regulatory requirement, it is effectively mandatory to avoid violation. Office of Foreign Assets Control, "Additional Questions from Financial Institutions."

35 Doubleday, "SSA Built a System to Help Combat Identity Fraud. Backers Say It's 'at Risk of Collapse'"; Eckerle, "When Failing an eCBSV Verification Isn't Indicative of Risk."

36 Galluzzo et al., "Attribute Validation Services for Identity Management: Architecture, Security, Privacy, and Operational Considerations."

37 Interviewees universally reported that these traditional methods are becoming less effective. One noted that a fraudster often has the victim's credit report in front of them when they are going through knowledge-based verification questions.

38 A 2023 Federal Reserve study found six percent of adults reported that neither they nor their partner had a checking, savings, or money market account. Board of Governors of the Federal Reserve System, "Economic Well-Being of U.S. Households in 2023," 35. A 2021 Federal Deposit Insurance Corporation survey found that five percent of households lacked checking or savings accounts, but results for 2023 had not been released at the time of publication. "2021 FDIC National Survey of Unbanked and Underbanked Households," 1.

39 "2021 FDIC National Survey of Unbanked and Underbanked Households," 2-3.

40 Rothschild, Novey, and Hanmer, "Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge"; 2021 FDIC National Survey of Unbanked and Underbanked Households," custom table generator.

41 Movement Advancement Project, "The ID Divide: How Barriers to ID Impact Different Communities and Affect Us All"; Fines and Fees Justice Center, "Free to Drive: End Driver's License Suspensions for Unpaid Fines and Fees"; Lindauer, "'Please Stop Telling Her to Leave.'"

42 Wang, "Are Generation Z Less Car-Centric Than Millennials?"; Wilson, "Zoomers Are Less Likely to Get Drivers Licenses — But They May Not Shift America's Transportation Culture."

43 Interviews with organizations that support individuals applying for ID found that lacking a birth certificate is a common roadblock for those struggling to assert their identity. See also Movement Advancement Project, "The ID Divide: How Barriers to ID Impact Different Communities and Affect Us All."

44 Interviews with nonprofits assisting unhoused populations obtain ID. See also "Why Laminating Your Birth Certificate Is Not a Good Idea."

45 This barrier is especially significant for those in rural areas. DMV closures may also disproportionately restrict access for Black individuals. For instance, the US Department of Transportation found that Alabama's attempted closure of 31 DMV offices in 2015 violated Title IV because of its disparate impact on Black communities. "U.S. Department of Transportation Takes Action to Ensure Equitable Driver License Office Access for Alabama Residents."

46 For instance, many US adults do not have their social security card, but there are no reliable studies that measure the extent of this problem.

47 Interviews with a variety of financial institutions.

48 Treasury Inspector General for Tax Administration, "Administration of the Individual Taxpayer Identification Number Program."

49 Although the IRS does not publicly release data. "A large proportion" is according to the IRS and Treasury Inspector General for Tax Administration. See Congressional Research Service, "Noncitizens and Eligibility for the 2020 Recovery Rebates."

50 Treasury Inspector General for Tax Administration, "Administration of the Individual Taxpayer Identification Number Program."

51 See: National Conference of State Legislatures, "States Offering Driver's Licenses to Immigrants"; American Immigration Council, "The Facts About the Individual Taxpayer Identification Number (ITIN)."

52 For a list of IDs accepted for ITIN applications, see Internal Revenue Service, "Instructions for Form W-7," 4.

53 Internal Revenue Service, "Acceptable Documents to Submit Your ITIN Application."

54 Treasury Inspector General for Tax Administration, "Administration of the Individual Taxpayer Identification Number Program."

55 Leisure, "ITIN's—What You Need to Know."

56 Max Blumenfeld, "Are ITINs Riskier than SSNs in Credit Card and Auto Lending? No."

57 For an overview of the history up to the COVID-19 pandemic, see Krajewska, "Implementing the REAL ID Act: Intergovernmental Conflict and Cooperation in Homeland Security Policy."

58 Physical security features for REAL IDs facilitate the detection of fake cards at three levels: cursory examination for rapid inspection at point of usage, examination by trained inspectors with simple equipment, and inspection by forensic specialists. The program additionally outlines standards for machine-readable information on the IDs. REAL ID also implements standards for the security of the issuance process itself. "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Extending Enforcement Date."

59 6 CFR 37.11.

60 In interviews, stakeholders revealed that training staff to validate multiple IDs was a major barrier to accepting more ID types and that a 20-40% turnover rate is common in bank branches.

61 See "IDNYC Banking Access Campaign"; "Banks & Credit Unions - IDNYC."

62 Won and Ramos, "Op-Ed: It's Time for New York Banks to Accept IDNYC."

63 Lovett, "New York State Wants Banks to Accept City Municipal ID Cards to Help Immigrants Wishing to Open an Account."

64 Board of Governors of the Federal Reserve System et al., "Letter to New York City and the New York Bankers Association," April 30, 2015.

65 The city's directory of FIs that accept the ID is out of date and has inaccuracies. For example, the page lists PNC Bank and First Republic Bank as accepting the ID as a primary form of identification. However, PNC Bank only accepts the card as a secondary ID alongside a driver's license, medicaid card, or other ID, and First Republic Bank is now part of JP Morgan Chase, which does not accept the ID. "Banks & Credit Unions - IDNYC."

66 Physical security features are physical characteristics of cards that make them more difficult to counterfeit. These can include high resolution photos, the cardholder's signature, embossing or engraving, reactions to ultraviolet light, micro-lettering in certain areas, etc. They can also include information transmitted via microchips and barcodes.

67 See "Document Calculator - How to Apply - IDNYC."

68 CDD typically refers to the ongoing monitoring of accounts rather than upfront KYC processes. See Section 4.1.

69 Faz, "Mexico's Tiered KYC: An Update on Market Response."

70 See Section 6.

71 U.S. Department of the Treasury, "Press Release: Final Rule for Electronic Government Payments Will Balance Recipient Needs with Benefits of Electronic Payment."

72 Cities for Financial Empowerment Fund, "Bank On."

73 DiVito, "Banking for All: How the USPS Could Provide Public Banking"; Friedline et al., "Postal Banking: How the United States Postal Service Can Partner on Public Options"; Baumann, "Postal Service Banking Limps On Despite Lackluster Results of Pilot Program."

74 Dayen, "USPS Begins Postal Banking Pilot Program"; Campaign for Postal Banking, "Support Postal Banking."

75 American Association of Motor Vehicle Administrators, "Jurisdiction Data Maps."

76 mDLs can be used to quickly prove someone's identity who has lost access to their physical ID card and can be renewed and updated very quickly compared to a physical ID.

77 For a more in-depth explanation, see Lord, "What Is Public Key Cryptography? (And How It Works)."

78 "ISO/IEC 18013-5:2021."

79 For a brief overview, see U.S. Department of the Treasury, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector."

80 FinRegLab interviews with an mDL administrator. See "ISO/IEC TS 18013-7: Life Cycle."

81 Bill Fisher, Fisher, "Check Your Wallet?"; National Institute of Standards and Technology, "Accelerating the Adoption of Mobile Driver's Licenses."

82 NIST NCCoE, "NCCoE Announces Collaborators | Mobile Driver's License (mDL) Project Use Case #1."

83 See American Association of Motor Vehicle Administrators, "Mobile Driver License Digital Trust Service."

84 National Institute of Standards and Technology, "Accelerating the Adoption of Mobile Driver's Licenses."

85 Rep. Foster, H.R.4258 Improving Digital Identity Act of 2021; Sen. Sinema, S.884 - 118th Congress (2023-2024): Improving Digital Identity Act of 2023.

86 There are several such proposals. For instance, Worldcoin, a cryptocurrency project backed by prominent venture capitalists, envisions a global network of digital IDs created with iris scans that allows users to securely transact in its cryptocurrency. "Worldcoin Whitepaper."

87 Consortia and non-profits that are working on standardization and interoperability issues include the OpenID Foundation, the Web3ID coalition, the Global Acceptance Network, and Trust Over IP (ToIP).

88 Dock, "Zero-Knowledge Proofs"; Land, "Lone Star Credit Union Successfully Pilots New BonifiID Identity Credential from Bonifii and GlobaliD."Dock, "Zero-Knowledge Proofs"; Land, "Lone Star Credit Union Successfully Pilots New BonifiID Identity Credential from Bonifii and GlobaliD." See also Box 19.

89 Banks are allowed to rely on certain other regulated FIs' performance of KYC functions where the parties have certain contractual arrangements and the reliance is reasonable under the circumstances. 31 C.F.R. § 1020.220(a)(6).

90 Smethurst, "Digital Identity Wallets and Their Semantic Contradictions"; Sovrin, "What Is Self-Sovereign Identity?"; Allen, "The Path to Self-Sovereign Identity."

91 Clark, Reid, and Labriolle, "Public-Private Cooperation to Build Digital Identity Systems."

92 Consortia and non-profits that are working with both the private and public sector on standardization and interoperability issues include the OpenID Foundation, the Global Acceptance Network, and Trust Over IP (ToIP).

93 Identity theft is a specific kind of fraud that uses the identifying information of another person without their authorization.

94 The information must be retained for 5 years. 31 CFR 1010.410.

95 These transactions are covered by the Electronic Fund Transfer Act and are therefore exempt from Travel Rule requirements. Financial Crimes Enforcement Network, "Funds 'Travel' Regulations: Questions & Answers."

96 Interviews with domestic financial institutions suggest this optional information on the recipient is generally included by US institutions.

97 31 CFR 1010.410(e).

98 31 CFR 1020.320.

99 31 CFR 1010.310-340.

100 Federal Deposit Insurance Corporation, "Connecting the Dots…The Importance of Timely and Effective Suspicious Activity Reports."

101 For instance, it would be out-of-pattern if a customer that only does small domestic transactions suddenly began making larger international transactions or suddenly began making transactions from a different location.

102 BSA defines "structuring" as when an individual conducts or attempts to conduct one or more transactions in currency in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading CTR filing requirements. 31 CFR 1010.100 (xx).

103 "FinCEN Suspicious Activity Report Electronic Filing Requirements Version 1.4."

104 Federal Financial Institutions Examination Council, "BSA/AML Manual / Assessing Compliance with BSA Regulatory Requirements / Currency Transaction Reporting."

105 Financial Crimes Enforcement Network, "Customer Due Diligence Requirements for Financial Institutions: Final Rules."

106 Other requirements include having a process to periodically update the program to detect and respond to new risks to customers and to the safety and soundness of the FI. The Red Flags Rule is enforced by the prudential regulators for banks and by the Federal Trade Commission for non-banks. 16 CFR Part 681.

107 15 U.S.C. §§ 1666-1666j, 1693a, 1693f, 1693g. U.C.C. § 4A.

108 Nasdaq Verafin, "Global Financial Crime Report: Insights at the Intersection of Financial Crime Data & Real Survivor Rates"; "Money Laundering Overview."

109 See LexisNexis, "True Cost of Financial Crime Compliance Study 2023: U.S. & Canada."

110 See Pol, "Anti-Money Laundering."

111 For instance, revealing details of a SAR filing is a criminal offense under the Bank Secrecy Act. 12 CFR 21.11.

112 "Getting to Effectiveness - Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance"; Ketenci et al., "A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering"; Oztas et al., "Transaction Monitoring in Anti-Money Laundering: A Qualitative Analysis and Points of View from Industry."

113 Anti-Money Laundering Act of 2020, section 6203(b)(1), Public Law 116-283, 134 Stat. 3388, 4568 (Jan. 1, 2021); 89 Fed. Reg. 55,429 (July 3, 2024).

114 Consumerist, "TransUnion Must Pay $60M For Mistakenly Tagging People As Possible Terrorists"; Camhi, "Regulatory Screening: False Positives and Their Customer Experience Impact."

115 See, e.g.: U.S. Government Accountability Office, "Anti-Money Laundering: Better Information Needed on Effectiveness of Federal Efforts"; Pol, "Anti-Money Laundering"; Basel Institute on Governance, "How Effective Are Jurisdictions at Preventing Money Laundering? Insights from the 10th Basel AML Index."

116 Financial Crimes Enforcement Network, "FinCEN Assesses Record $1.3 Billion Penalty against TD Bank."

117 The FTC received almost 2.6 million fraud reports, and losses totaled over $10 billion in 2023, compared to almost 2.5 million fraud reports with losses of only $3.5 billion in 2020. Federal Trade Commission, "Fraud Reports."

118 First-party fraud includes applicants misrepresenting their income on an application for credit, applying for a loan that they do not intend to pay back, and account holders falsely claiming that a transaction was fraudulent to seek reimbursement from their FI.

119 12 C.F.R. §§ 1005.2(m), 1005.3(c)(3), 1005.6.

120 Bourke, "Stopping Scams Against Consumers"; U.S. Government Accountability Office, "Payment Scams: Information on Financial Industry Efforts."

121 "Aspen FSP Launches National Task Force for Fraud & Scam Prevention."

122 For example, one financial institution revealed in an interview that when a fraudster is going through knowledge-based verification questions they often have the victim's credit report in front of them. Moreover, legitimate consumers often do not know the answers to these questions, which can range from previous addresses to exact mortgage payment amounts (including changing monthly totals in escrow).

123 The SAR threshold is $5,000 for most FIs and $2,000 for MSBs. See Section 4.1.

124 Oztas et al., "Transaction Monitoring in Anti-Money Laundering: A Qualitative Analysis and Points of View from Industry."

125 Braun et al., "Understanding Risk Management in Emerging Retail Payments"; Spiotto, "Credit, Debit, or ACH: Consequences & Liabilities A Comparison of the Differences in Consumer Liabilities"; Karkal, "How to Fight Growing ACH Fraud."

126 Lumley, "US Real-Time Payments Are in Their Early Days, but Show Steady Growth"; Chen, "Banks"; FRB Services, "Fraud and Instant Payments: The Basics."

127 PYMNTS, "Jack Henry Debuts Defense Against Money Laundering"; "AI Innovation Explored: Insights into AI Applications in Financial Services and Housing." (Frederick Reynolds of FIS reporting their prototyping of generative AI for fraud defense shows that the technology can reduce false positives significantly). See Box 16 for further discussion of generative AI.

128 "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector," sec. 6.2.

129 See, e.g., PYMNTS, "A False Declined Payment Costs Merchants More Than a Sale"; PYMNTS, "Nearly 60% of Firms Say Failed Payments Are Expensive to Track and Resolve"; PYMNTS, "Deep Dive: How Merchants Can Reduce the Risk of False Positives Through AI and ML."

130 Javelin Research, "Overcoming False Positive Declines in E-Commerce"; Taxpayer Advocate Service, "Reducing 'False Positive' Determinations in Fraud Detection"; ClearSale, "State of Consumer Attitudes on Ecommerce, Fraud & CX 2021"; ClearSale, "Original Research Report 2024: Ecommerce False Declines & Consumer Behavior"; "2022 IBM Global Financial Fraud Impact Report."

131 See also San Francisco Office of Financial Empowerment, "Blacklisted: How ChexSystems Contributes to Systemic Financial Exclusion," 10 (recounting the experience of a consumer whose account was closed after a government agency in another state accidentally routed funds to his account and then tried to claw them back).

132 Consumer Financial Protection Bureau, "Consent Order in the Matter of Wells Fargo Bank, N.A."

133 Kessler, "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money"; McGreevy, "Bank of America Must Provide More Proof of Fraud before Freezing EDD Accounts, Court Orders"; Consumer Financial Protection Bureau, "Federal Regulators Fine Bank of America $225 Million Over Botched Disbursement of State Unemployment Benefits at Height of Pandemic."

134 Federal AML guidance states that the filing of a SAR "on its own, should not be the basis for terminating a customer relationship," but rather that FIs must make their own determination about whether to close accounts in light of the facts and circumstances. Financial Crimes Enforcement Network, "Answers to Frequently Asked Bank Secrecy Act (BSA) Questions," question 6. Some stakeholders report that they have been told by law enforcement officials that keeping accounts open can often be beneficial while investigations are ongoing, but that FIs often believe that banking regulators prefer for accounts to be shut down to minimize risk to the institution.

135 "Getting to Effectiveness - Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance."

136 Clements, "Further Actions Needed to Address Domestic and International Derisking Concerns."

137 15 U.S.C. §§ 1691(d), 1681m(a), (b), (h), 1681a(k)(1); 12 CFR §§ 1002.9, 1022.72. Although sample reasons are provided in an appendix to federal fair lending regulations, they do not address situations involving fraud or AML concerns in detail. 12 C.F.R. Pt. 1002, App. C. The Consumer Financial Protection Bureau entered a consent decree with a bank in 2023 over its provision of adverse action notices stating that credit card applications had been denied "due to possible credit abuse," where bank employees were declining applicants with Armenian names because they suspected an Armenian fraud ring was operating in southern California. Consumer Financial Protection Bureau, "Consent Order in the Matter of Citibank, N.A."

138 15 U.S.C. §§ 1681m(a), 1681a(k)(1); 12 CFR § 1022.72.

139 See, e.g., Sanchez-Adams, "Testimony before the U.S. Senate Committee on Banking, Housing, and Urban Affairs: Examining Scams and Fraud in the Banking System and Their Impact on Consumers."

140 Office of the Comptroller of the Currency, "Can the Bank Close My Checking Account and Not Notify Me?"

141 31 U.S.C. 5318(g)(2); 31 C.F.R. § 1020.320(e).

142 Trew, "Closing the Book on Account Closures."

143 Office of the Comptroller of the Currency, "Can the Bank Close My Checking Account and Not Notify Me?"

144 Sanchez-Adams, "Testimony before the U.S. Senate Committee on Banking, Housing, and Urban Affairs: Examining Scams and Fraud in the Banking System and Their Impact on Consumers."

145 Kessler, "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money"; McGreevy, "Bank of America Must Provide More Proof of Fraud before Freezing EDD Accounts, Court Orders"; Consumer Financial Protection Bureau, "Federal Regulators Fine Bank of America $225 Million Over Botched Disbursement of State Unemployment Benefits at Height of Pandemic"; "CFPB Orders U.S. Bank to Pay $21 Million for Illegal Conduct During COVID-19 Pandemic."

146 San Francisco Office of Financial Empowerment, "Blacklisted: How ChexSystems Contributes to Systemic Financial Exclusion." Overall, about 13.6 percent of households that did not have bank accounts in the FDIC's most recent survey on bank account usage reported that their lack of access is due in part to problems with past banking or credit history, although the survey did not differentiate between different types of historical problems. Demirguc-Kunt et al., "The Global Findex Database 2021"; "2021 FDIC National Survey of Unbanked and Underbanked Households."

147 Consumer Financial Protection Bureau, "Helping Consumers Who Have Been Denied Checking Accounts."

148 San Francisco Office of Financial Empowerment, "Blacklisted: How ChexSystems Contributes to Systemic Financial Exclusion."

149 Whelehan, "What Is ChexSystems?"

150 Crossman, "Rushed Anti-Money-Laundering Calls Backfire. Can AI Help?"

151 Bernard and Lieber, "Banks Are Closing Customer Accounts, With Little Explanation"; Lieber and Bernard, "Why Banks Are Suddenly Closing Down Customer Accounts"; Trew, "Closing the Book on Account Closures."

152 "Serving Communities of Color: A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color," 40; Morgan, "Financial Fraud in the United States, 2017"; Medintz, "Black and Latino Consumers Are More Likely to Lose Money to Digital Scams, a Consumer Reports Study Finds"; AARP Research, "The Fraud Crisis in America: How Adult Consumers Feel, What They Know, and Their Actions That Pose Risks"; DeLiema and Witt, "Profiling Consumers Who Reported Mass Marketing Scams: Demographic Characteristics and Emotional Sentiments Associated with Victimization." The Identity Theft Resource Center reports that 61 percent of victims that sought help from the organization in 2022 were women, and victims that contacted the organization were more likely to be Black than the general population. See Identity Theft Resource Center, "2023 Consumer Impact Report," 2023, 5 and Identity Theft Resource Center, "Identity in Practice Report: Understanding Identity Crimes in Black Communities."

153 DeLiema et al., "Exposed to Scams: What Separates Victims from Non-Victims?"; Hanoch and Wood, "The Scams Among Us: Who Falls Prey and Why."

154 DeLiema et al., "Exposed to Scams: What Separates Victims from Non-Victims?"; Hanoch and Wood, "The Scams Among Us: Who Falls Prey and Why"; Federal Bureau of Investigation Internet Crime Complaint Center, "Elder Fraud Report 2023"; Morgan and Tapp, "Examining Financial Fraud Against Older Adults."

155 The Federal Financial Institutions Examination Council, a federal interagency body that makes guidelines for regulators' examinations of FIs, notes that international funds transfers and cross-border ACH transactions are particularly high risk and should be subject to greater scrutiny for potential OFAC violations. Federal Financial Institutions Examination Council, "BSA/AML Manual / Office of Foreign Assets Control."

156 Federal Financial Institutions Examination Council.

157 See, e.g., Jeydel, Hayes, and Egan, "OFAC Asserts Jurisdiction over French Banks's Internal Transfers and Foreign Exchange Transactions."

158 "The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation."

159 The Financial Action Task Force, "Countries."

160 The FATF found the US noncompliant with R.22, R.23, and R.28 in 2023, and all of these deficiencies stem from a lack of oversight of "Designated Non-Financial Businesses and Professions (DNFBPs)," which include real estate agents and dealers in precious metals and stones. The Financial Action Task Force, "United States: 7th Follow-Up Report & Technical Compliance Re-Rating."

161 See The Financial Action Task Force, "High-Risk and Other Monitored Jurisdictions."

162 The "black list" is reserved for countries with severe noncompliance and no political commitment to come into compliance. These countries are Iran, Myanmar, and the Democratic People's Republic of Korea.

163 Several multinational financial institutions brought up this issue in our interviews.

164 See Section 4.1 above.

165 See, e.g., Gegory, "FinCEN: Docket Number FINCEN-2020-0002; RIN 1506-AB41 Board: Docket Number R-1726; RIN 7100-AF97," November 27, 2020.

166 The risk avoided could relate to fraud or money laundering, but de-risking is most commonly discussed in the context of illicit finance. The World Bank Group, "De-Risking in the Financial Sector"; United States Department of State, "De-Risking."

167 See "The Department of the Treasury's De-Risking Strategy."

168 "The Department of the Treasury's De-Risking Strategy."

169 See, e.g., National Iranian American Council, "Memo: Ending Discriminatory Bank Account Closures."

170 "Consumer Financial Data: Legal and Regulatory Landscape."

171 H.R.8152 - American Data Privacy and Protection Act.

172 H.R.8818 - American Privacy Rights Act of 2024; Klar, "Data Privacy Bill Markup Canceled after House Leadership Opposition."

173 15 U.S.C. 1681, 1681a(d) & (f), 1681b.

174 "Consumer Financial Data: Legal and Regulatory Landscape"; FinRegLab, "Explainability & Fairness in Machine Learning for Credit Underwriting: Policy Analysis"; FinRegLab, "Explainability & Fairness in Machine Learning for Credit Underwriting: Policy & Empirical Findings Overview"; FinRegLab, "Machine Learning Explainability & Fairness: Insights from Consumer Lending." 81-107.

175 5 U.S.C. §§ 1681m(a), (b), (h), 1681a(k)(1); 12 CFR § 1022.72.

176 GLBA imposes privacy and security protections on consumers' financial data but does not address issues such as accuracy. "Consumer Financial Data: Legal and Regulatory Landscape"; FinRegLab, "Explainability & Fairness in Machine Learning for Credit Underwriting: Policy Analysis"; FinRegLab, "Explainability & Fairness in Machine Learning for Credit Underwriting: Policy & Empirical Findings Overview"; FinRegLab, "Machine Learning Explainability & Fairness: Insights from Consumer Lending." 46-80. GLBA coverage was litigated between TransUnion, the Federal Trade Commission, and other parties two decades ago, but at the time all of the litigants agreed that credit header data was not a consumer report under the FCRA so federal courts did not rule on the issue. Ellen Segal Huvelle, Individual Reference Services Group, Inc. and TransUnion LLC v. Federal Trade Commission, et al. Trans Union LLC v. Federal Trade Commission, 295 F.3d 42 (D.C. Cir. 2002).

177 See Wiley, "What Is Header Data?"

178 See, e.g., Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability."

179 Consumer Financial Protection Bureau, "Small Business Advisory Review Panel for Consumer Reporting Rulemaking: Outline of Proposals and Alternatives Under Consideration"; National Consumer Law Center, "Letter from Coalition of Immigrant, Consumer, and Privacy Groups Urging CFPB to Use FCRA to Rein in Data Brokers."

180 "Comment from CFPB (TREAS-DO-2024-0011-0001)."

181 Vittorio and Weinberger, "Sales of Personal Data on Consumer Credit Reports Draw Scrutiny"; Shelley Thompson, "Re: Forthcoming CFPB 'Data Broker' Rulemaking under the FCRA"; Chris Willis, "The Consumer Finance Podcast: Exploring the CFPB's Stance on AI in Financial Services."

182 The Equal Credit Opportunity Act prohibits discrimination in "any aspect" of a credit transaction on various grounds including race, ethnicity, and gender. 15 U.S.C. § 1691(a). The law has generally been interpreted not only to prohibit including such protected characteristics in credit models but to prohibit the use of other criteria that may have a disproportionately negative impact on protected groups, unless the criteria meet a legitimate business need that cannot reasonably be achieved through means that have less of a "disparate impact." As a result, many lenders test potential variables to determine their impact on different demographic groups relative to their importance in predicting loan defaults.

183 "Comment from CFPB (TREAS-DO-2024-0011-0001)."

184 "CFPB Targets Unfair Discrimination in Consumer Finance"; Chamber of Commerce vs. Consumer Financial Protection Bureau, No. 6:22-cv-00381, Opinion and Order (E.D. Tex. Sept. 8, 2023).

185 For example, use of personal information on such topics as age to confirm identity may raise different concerns than using such information in the context of predicting credit risks and guarding against discrimination.

186 Consumer Financial Protection Bureau, "Required Rulemaking on Personal Financial Data Rights."

187 See, e.g., Azevedo, "Exclusive: Plaid, Once Aimed Mostly at Fintechs, Is Growing Its Enterprise Business and Now Has over 1,000 Customers Signed On"; Yodlee, "Bank Identity Verification | Verify Customer Account Holder Details"; MX, "Secure, Instant Identity and Account Verifications"; Finicity, "Instant Bank Account Verification | Account Owner Validation."

188 12 C.F.R. § 1033.211(f).

189 Forcht Bank, N.A., Kentucky Bankers Association, and Bank Policy Institute v. Consumer Financial Protection Bureau.

190 See generally Consumer Financial Protection Bureau, "Small Business Advisory Review Panel for Consumer Reporting Rulemaking: Outline of Proposals and Alternatives Under Consideration." The CFPB stated in the course of the open banking rulemaking that it considered data aggregators to be consumer reporting agencies under certain circumstances. 88 Fed. Reg. 74,796, 74,801 (Oct. 31, 2023). However, the final rule leaves such determinations to the FCRA proceeding, CFPB, "Notice of Final Rulemaking - Required Rulemaking on Personal Financial Data Rights."

191 For instance, FICO released Falcon, a neural network-based anti-fraud product in 1992. See also T.J. Horan, "Evolution of Fraud Analytics - An Inside Story."

192 See, e.g., Oztas et al., "Transaction Monitoring in Anti-Money Laundering: A Qualitative Analysis and Points of View from Industry."

193 See, e.g., Afriyie et al., "A Supervised Machine Learning Algorithm for Detecting and Predicting Fraud in Credit Card Transactions." "Project Aurora: The Power of Data, Technology, and Collaboration to Combat Money Laundering across Institutions and Borders," sec. 4.3. See also Fitzgerald, "Inside FIS' Use of AI to Weed out False-Positive Card Fraud Alerts."

194 Oztas et al., "Transaction Monitoring in Anti-Money Laundering: A Qualitative Analysis and Points of View from Industry."

195 For example, MasterCard has indicated that it is using generative AI to analyze partial credit card numbers posted on illegal websites by card skimmers who are attempting to sell information to fraudsters. Based on the predicted full card number, it is alerting FIs that the cards may have been compromised. Visa has reported that it uses elements of generative AI to create a risk score that predicts the likelihood that seemingly innocuous transactions are part of "enumeration attacks" that will soon escalate into larger fraud attempts. Ryan Browne, Browne, "Mastercard Jumps into Generative AI Race with Model It Says Can Boost Fraud Detection by up to 300%"; Wodecki, "Visa Uses Generative AI to Catch Suspicious Financial Transactions."

196 Kakkad et al., "A Survey on Explainability of Graph Neural Networks."

197 "Projects: Project Aurora."

198 See, e.g., Bakry et al., "Automatic Suppression of False Positive Alerts in Anti-Money Laundering Systems Using Machine Learning"; Vorobyev and Krivitskaya, "Reducing False Positives in Bank Anti-Fraud Systems Based on Rule Induction in Distributed Tree-Based Models." See also KPMG and nets, "Fighting Fraud with a Model of Models."

199 For generative AI use in the production of fake IDs, see, e.g., Cox, "An Instant Fake ID Factory."

200 The lack of security of voice authentication systems has been raised by the Senate Banking Committee and has been echoed by industry stakeholders that FinRegLab has interviewed. United States Committee on Banking, Housing, and Urban Affairs, "Brown Presses Banks on Voice Authentication Services."

201 "Leveraging Generative AI (GenAI) for Fraud Detection and Prevention"; "Synthetic Data Generation"; Browne, "Mastercard Jumps into Generative AI Race with Model It Says Can Boost Fraud Detection by up to 300%"; Wodecki, "Visa Uses Generative AI to Catch Suspicious Financial Transactions."

202 See, e.g., Leffer, "AI Audio Deepfakes Are Quickly Outpacing Detection"; Jingnan, "Using AI to Detect AI-Generated Deepfakes Can Work for Audio — but Not Always."

203 See Qi et al., "DeepRhythm." For further discussion of different types of liveness tests, see Faceplugin, "Active Liveness Detection vs Passive Liveness Detection."

204 Interviews with stakeholders. See also Cox, "An Instant Fake ID Factory."

205 "Consumer Financial Data: Legal and Regulatory Landscape"; FinRegLab, "Explainability & Fairness in Machine Learning for Credit Underwriting: Policy Analysis"; FinRegLab, "Explainability & Fairness in Machine Learning for Credit Underwriting: Policy & Empirical Findings Overview"; FinRegLab, "Machine Learning Explainability & Fairness: Insights from Consumer Lending."

206 "Artificial Intelligence Act" (adopting a negotiating position ahead of final talks with member nations); "Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence"; "Building Trust in Human Centric Artificial Intelligence."

207 "Artificial Intelligence Act" (seven qualities: valid/ reliable, safe, secure/resilient, explainable/interpretable, privacy-enhanced, fair/ harmful bias managed, accountable/transparent); Organisation for Economic Co-operation and Development, "Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence" (six key principles: inclusive growth, sustainable development and well-being; human-centered values and fairness; transparency and explainability; robustness, security and safety; and accountability); Ostmann and Dorobantu, "AI in Financial Services" (five principles of AI ethics, which include fairness, sustainability, safety, accountability, and transparency); see also Stanton and Jensen, "Trust and Artificial Intelligence (Draft)" (discussing nine qualities: accuracy, reliability, resiliency, objectivity, security, explainability, safety, accountability, and privacy).

208 Bank Service Company Act, 12 U.S.C. §§ 1661–1867(c); 12 U.S.C. §§ 5514–5516; "Compliance Bulletin and Policy Guidance; 2016-02, Service Providers."

209 "Consumer Financial Data: Legal and Regulatory Landscape."

210 For this reason, large banks are often more willing to work with outside vendors than in other contexts such as credit underwriting, where they tend to build and rely upon their own models.

211 See U.S. Department of the Treasury, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector," sec. 2.5.

212 McCaffrey, "ABA to Launch Information-Sharing Exchange to Help Banks Fight Fraud."

213 Azevedo, "When Foes Become Friends: Capital One Partners with Fintech Giants Stripe, Adyen to Prevent Fraud."

214 See Financial Crimes Enforcement Network, "Section 314(b) Fact Sheet." Financial Institutions must register with FinCEN before sharing data.

215 See Pape, "Sharing Fraud Data Is Hard. Two Industry Efforts Aim to Make It Easier."

216 Financial Crimes Enforcement Network, "Section 314(b) Fact Sheet."

217 U.S. Department of the Treasury; Pape, "Treasury Accuses Banks of 'Insufficient Data Sharing' on Fraud."

218 In contrast, nearly 300,000 financial institutions and other companies have registered to provide electronic AML reports to the federal government. "Financial Crimes Enforcement Network (FinCEN) Year in Review for FY 2023"; Bethencourt, "Changes in Bank Regulations, Financial Compliance Regulations, Regulation Banks, Money Laundering Cases, Anti Money Laundering, Money Laundering Training."

219 See Box 19.

220 The most relevant example of standardizing data formats is ISO20022, which is particularly promising in the context of cross-border payments. See "About ISO 20022." ISO20022 is a voluntary payment messaging standard developed by the International Organization for Standardization, which many FIs have adopted to ensure uniformity in information included with payments. This standardization drives operating efficiency and prevents the loss of information with transactions by eliminating the need for translation between disparate payment messaging formats. The standard is also used by the Federal Reserve's FedNow Service for instant payments that launched in 2023.

221 The Bank for International Settlements found that AML/CFT false positives were reduced substantially with data sharing in combination with employing more complex analytics. See "Project Aurora: The Power of Data, Technology, and Collaboration to Combat Money Laundering across Institutions and Borders."

222 See IBM Research, "What Is Federated Learning?"; FinRegLab, "Assessing Federated Machine Learning's Potential for Transforming KYC/AML."

223 See "Project Aurora: The Power of Data, Technology, and Collaboration to Combat Money Laundering across Institutions and Borders," sec. 4.2 part A. Homomorphic encryption is a technique that allows the computation of encrypted data without having to first decrypt it. Local differential privacy adds a certain amount of "noise" to obfuscate data to make it more difficult to link it to individuals.

224 Ludwig and Baracaldo, "Federated Learning: A Comprehensive Overview of Methods and Applications."; Sen, Waghela, and Rakshit, "Privacy in Federated Learning"; "Projects: Project Aurora."

225 Shoemaker, "What Are Decentralized Identifiers (DIDs)?"; Coinbase, "What Is a Decentralized Identifier (DID)?"; Sharma and Lloyd, "Empowering Constituents through Web3: A Vision for Personal Financial Data Rights"; Chainlink, "Zero-Knowledge Proof (ZKP) — Explained"; Sporny et al., "Verifiable Credentials Data Model v2.0."

226 See Sharma and Lloyd, "Empowering Constituents through Web3: A Vision for Personal Financial Data Rights"; Chainlink, "Zero-Knowledge Proof (ZKP) — Explained"; Sporny et al., "Verifiable Credentials Data Model v2.0."

227 IBM, "IBM Completes Proof-of-Concept Blockchain-Based Shared KYC"; Tweeddale, "Introducing the First Regulatory Compliant, Reusable KYC/KYB Digital Credential Solution"; "Project VISH Verification Info Sharing Hub Proof of Concept (POC)."

228 See, e.g., Askin et al., "Trust in a Trustless System."

229 Jensen et al., "A Synthetic Data Set to Benchmark Anti-Money Laundering Methods."

230 "Digital Identities - mDL | NCCoE."

231 HM Treasury, "The Payment Services (Amendment) Regulations 2024: Policy Note."

232 R.16 concerns "wire transfers," but the proposed revisions would instead adopt the terminology "payment or value transfer" to be platform neutral.

233 The Financial Action Task Force, "Public Consultation on Recommendation 16 on Payment Transparency." See also "About ISO 20022."

234 This is in line with ISO20022 as well. See The Bank for International Settlements, "Report to the G20: Harmonised ISO 20022 Data Requirements for Enhancing Cross-Border Payments."

235 For instance, the average monthly remittance to Mexico from the US was $390 in 2022. This number is likely much lower for individuals with low income and little documentation. Cañas and Pranger, "Strong U.S. Labor Market Drives Record Remittances to Mexico." It should also be noted that the FATF allows the threshold for these information requirements to be set lower than $1,000, yet doing so is uncommon.

236 De-risking refers to when FIs terminate or restrict relationships with customers or categories of customers to avoid risk rather than assessing and managing it appropriately. De-risking is a major driver of exclusion in remittances and cross-border payments, where FIs refuse to complete transactions with countries that carry higher AML risk or serve customers in those countries more broadly.

237 See Jeník, Kerse, and De Koker, "FATF's Proposed Rules for Payments: Balancing Integrity and Inclusion?"

238 These transactions typically present lower illicit finance risk because cardholders are customers of FIs that are contractually obligated by card networks to adhere to AML/CFT compliance measures. The Financial Action Task Force, "Public Consultation on Recommendation 16 on Payment Transparency," 2.

239 Boyce and Jiang, "Can You Hear Us? Voices from Informal Businesses."

240 This would also remove exemptions for virtual assets and digital currencies because they are "cash equivalents." The Financial Action Task Force, "Public Consultation on Recommendation 16 on Payment Transparency," 4. Under Option 2, cross-border withdrawals would be subject to basic R.16 information requirements, which are relaying with a payment the name of the originator; the name of the beneficiary, and an account number for each, or a unique transaction reference number. Domestic withdrawals under $1,000 would be exempt from even these basic requirements. The additional information requirements for transactions above a country's threshold (typically $1,000) would still apply to both domestic and cross-border transactions, however.

241 See The Bank for International Settlements, "Report to the G20: Harmonised ISO 20022 Data Requirements for Enhancing Cross-Border Payments."

242 See Jeník, Kerse, and De Koker, "FATF's Proposed Rules for Payments: Balancing Integrity and Inclusion?"; Koker, "Editorial: Regulatory Impact Assessment: Towards a Better Approach for the FATF."

Bibliography

"2021 FDIC National Survey of Unbanked and Underbanked Households." Federal Deposit Insurance Corporation, October 2022. https://www.fdic.gov/household-survey.

"2022 IBM Global Financial Fraud Impact Report." Morning Consult, February 15, 2022. https://filecache.mediaroom.com/mr5mr_ibmnewsroom/193031/MC%20%2B%20IBM%20Financial%20Fraud%20Study%20-%20Global%20Report%20Updated%203.8.22.pdf.

"2023 Consumer Impact Report." Identity Theft Resource Center, 2023.

AARP Research. "The Fraud Crisis in America: How Adult Consumers Feel, What They Know, and Their Actions That Pose Risks." AARP, May 2024. https://doi.org/10.26419/res.00788.001.

Abraham, Jorij, Marianne Junger, James Greening, Luka Koning, Clement Njoki, and Sam Rogers. "The State of Scams in the United States of America." Global Anti-Scam Alliance, 2017. https://www.gasa.org/_files/ugd/7bdaac_ded603440c464fce97f4adde8f3f7f14.pdf.

Afriyie, Jonathan Kwaku, Kassim Tawiah, Wilhemina Adoma Pels, Sandra Addai-Henne, Harriet Achiaa Dwamena, Emmanuel Odame Owiredu, Samuel Amening Ayeh, and John Eshun. "A Supervised Machine Learning Algorithm for Detecting and Predicting Fraud in Credit Card Transactions." *Decision Analytics Journal* 6 (March 1, 2023): 100163. https://doi.org/10.1016/j.dajour.2023.100163.

"AI Innovation Explored: Insights into AI Applications in Financial Services and Housing," July 23, 2024. https://www.youtube.com/watch?v=s85zZ_9VLd4.

Allen, Christopher. "The Path to Self-Sovereign Identity." Life With Alacrity, April 26, 2016. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/.

American Association of Motor Vehicle Administrators. "Jurisdiction Data Maps." American Association of Motor Vehicle Administrators - AAMVA. Accessed August 5, 2024. https://www.aamva.org/jurisdiction-data-maps#anchorformdlmap.

———. "Mobile Driver License Digital Trust Service." American Association of Motor Vehicle Administrators - AAMVA. Accessed August 5, 2024. https://www.aamva.org/identity/mobile-driver-license-digital-trust-service.

American Immigration Council. "The Facts About the Individual Taxpayer Identification Number (ITIN)." American Immigration Council, March 14, 2022.

Anderson, Keith B. "To Whom Do Victims of Mass-Market Consumer Fraud Complain?" SSRN Scholarly Paper. Rochester, NY, May 24, 2021. https://doi.org/10.2139/ssrn.3852323.

Azevedo, Mary Ann. "Exclusive: Plaid, Once Aimed Mostly at Fintechs, Is Growing Its Enterprise Business and Now Has over 1,000 Customers Signed On." TechCrunch, June 29, 2024. https://techcrunch.com/2024/06/29/as-plaid-matures-the-fintech-giant-says-enterprise-growth-is-starting-to-outpace-the-rest-of-its-business/.

———. "When Foes Become Friends: Capital One Partners with Fintech Giants Stripe, Adyen to Prevent Fraud." TechCrunch, June 5, 2024. https://techcrunch.com/2024/06/05/when-foes-become-friends-capital-one-partners-with-fintech-giants-stripe-adyen-to-prevent-fraud/.

Bakry, Ahmed N., Almohammady S. Alsharkawy, Mohamed S. Farag, and K. R. Raslan. "Automatic Suppression of False Positive Alerts in Anti-Money Laundering Systems Using Machine Learning." *The Journal of Supercomputing* 80, no. 5 (March 1, 2024): 6264–84. https://doi.org/10.1007/s11227-023-05708-z.

Basel Institute on Governance. "How Effective Are Jurisdictions at Preventing Money Laundering? Insights from the 10th Basel AML Index." Basel Institute on Governance, October 2021. https://baselgovernance.org/blog/how-effective-are-jurisdictions-preventing-money-laundering-insights-10th-basel-aml-index.

Bernard, Tara Siegel, and Ron Lieber. "Banks Are Closing Customer Accounts, With Little Explanation." *The New York Times*, April 8, 2023, sec. Your Money. https://www.nytimes.com/2023/04/08/your-money/bank-account-suspicious-activity.html.

Bethencourt, Daniel. "Changes in Bank Regulations, Financial Compliance Regulations, Regulation Banks, Money Laundering Cases, Anti Money Laundering, Money Laundering Training." MoneyLaundering.com, October 8, 2021. https://www.moneylaundering.com/news/large-us-banks-sharing-financial-intelligence-through-private-exchange/.

Better Identity Coalition. "Better Identity in America: A Blueprint for State Policymakers," December 2022. https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/63937744d04cfd3dfa8d9838/1670608710401/Better_Identity_Coalition+-+State+Blueprint+-+Dec2022.pdf.

BIS. "Projects: Project Aurora," March 27, 2024. https://www.bis.org/about/bisih/topics/fmis/aurora.htm.

Board of Governors of the Federal Reserve System. "Economic Well-Being of U.S. Households in 2022." Board of Governors of the Federal Reserve System, May 2023.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, and Office of the Comptroller of the Currency. "Letter to New York City and the New York Bankers Association," April 30, 2015. https://www.scribd.com/document/272763771/BdofGovsLetter.

Bourke, Nick. "Stopping Scams Against Consumers: Roadmap for a National Strategy." SSRN Scholarly Paper. Rochester, NY, July 22, 2024. https://doi.org/10.2139/ssrn.4897644.

Boyce, Taylor, and Charlotte Nan Jiang. "Can You Hear Us? Voices from Informal Businesses." *Let's Talk Development* (blog), August 24, 2023. https://blogs.worldbank.org/en/developmenttalk/can-you-hear-us-voices-informal-businesses.

Braun, Michele, James McAndrews, William Roberds, and Richard J. Sullivan. "Understanding Risk Management in Emerging Retail Payments." *Federal Reserve Bank of New York Economic Policy Review*, September 2008. https://doi.org/10.2139/ssrn.1072914.

Browne, Ryan. "Mastercard Jumps into Generative AI Race with Model It Says Can Boost Fraud Detection by up to 300%." CNBC, February 1, 2024. https://www.cnbc.com/2024/02/01/mastercard-launches-gpt-like-ai-model-to-help-banks-detect-fraud.html.

Camhi, Jonathan. "Regulatory Screening: False Positives and Their Customer Experience Impact." *Bank Systems & Technology*, April 30, 2014. https://www.banktech.com/regulatory-screening-false-positives-and-their-customer-experience-impact/d/d-id/../../../risk-management/regulatory-screening-false-positives-and/240168061.

Campaign for Postal Banking. "Support Postal Banking." Campaign for Postal Banking, July 14, 2023. https://www.campaignforpostalbanking.org/.

Cañas, Jesus, and Ana Pranger. "Strong U.S. Labor Market Drives Record Remittances to Mexico." Federal Reserve Bank of Dallas, October 20, 2023. https://www.dallasfed.org/research/swe/2023/swe2310.

Chainlink. "Zero-Knowledge Proof (ZKP) — Explained." Chainlink, July 29, 2024. https://chain.link/education/zero-knowledge-proof-zkp.

Chen, Jeremy. "Banks: Real-Time Fraud Considerations to Maximize the Benefits." Finextra Research, July 27, 2023. https://www.finextra.com/blogposting/24641/banks-real-time-fraud-considerations-to-maximize-the-benefits.

Chris Willis. "The Consumer Finance Podcast: Exploring the CFPB's Stance on AI in Financial Services," September 26, 2024. https://www.troutman.com/a/web/wCTmPsqGJ5w9hNx8D5VhY7/transcript_cfp_exploring_the_cfpbs_stance_on_ai_in_financial_services.pdf.

Cities for Financial Empowerment Fund. "Bank On." Cities for Financial Empowerment Fund, July 18, 2016. https://cfefund.org/project/bank-on/.

Clark, Julia, Kyla Reid, and Stéphanie de Labriolle. "Public-Private Cooperation to Build Digital Identity Systems." World Bank Blogs, July 26, 2016. https://blogs.worldbank.org/en/digital-development/public-private-cooperation-build-digital-identity-systems.

ClearSale. "Original Research Report 2024: Ecommerce False Declines & Consumer Behavior." ClearSale, 2024. https://en.clear.sale/hubfs/eBook_Ecommerce%20False%20Declines%20%26%20Consumer%20Behavior%20Guide_v1.pdf.

———. "State of Consumer Attitudes on Ecommerce, Fraud & CX 2021." ClearSale, 2022. https://www2.clear.sale/consumer-behavior-intro.

Clements, Michael E. "Further Actions Needed to Address Domestic and International Derisking Concerns." United States Government Accountability Office, June 26, 2018. https://www.gao.gov/assets/gao-18-642t.pdf.

Coinbase. "What Is a Decentralized Identifier (DID)?" coinbase. Accessed September 27, 2024. https://www.coinbase.com/learn/wallet/what-is-a-decentralized-identifier-did.

"Comment from CFPB (TREAS-DO-2024-0011-0001)." The Department of the Treasury, August 12, 2024. https://www.regulations.gov/comment/TREAS-DO-2024-0011-0069.

"Compliance Bulletin and Policy Guidance; 2016-02, Service Providers." Consumer Financial Protection Bureau, October 31, 2016. https://www.consumerfinance.gov/compliance/supervisory-guidance/compliance-bulletin-and-policy-guidance-2016-02-service-providers/.

Congressional Research Service. "Noncitizens and Eligibility for the 2020 Recovery Rebates." Congressional Research Service, May 1, 2020. https://crsreports.congress.gov/product/pdf/IN/IN11376.

"Consumer Financial Data: Legal and Regulatory Landscape." Financial Health Network, Flourish, FinRegLab, and Mitchell Sandler, n.d. https://finreglab.org/research/consumer-financial-data-legal-and-regulatory-landscape/.

Consumer Financial Protection Bureau. "CFPB Orders U.S. Bank to Pay $21 Million for Illegal Conduct During COVID-19 Pandemic," December 19, 2023. https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-us-bank-to-pay-21-million-for-illegal-conduct-during-covid-19-pandemic/.

Consumer Financial Protection Bureau. "CFPB Targets Unfair Discrimination in Consumer Finance," March 16, 2022. https://www.consumerfinance.gov/about-us/newsroom/cfpb-targets-unfair-discrimination-in-consumer-finance/.

Consumer Financial Protection Bureau. "Consent Order in the Matter of Citibank, N.A." Consumer Financial Protection Bureau, November 8, 2023. https://files.consumerfinance.gov/f/documents/cfpb_citibank-na_2023-cfpb-0013_consent-order_2023-11.pdf.

———. "Consent Order in the Matter of Wells Fargo Bank, N.A." Consumer Financial Protection Bureau, December 20, 2022. https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

———. "Federal Regulators Fine Bank of America $225 Million Over Botched Disbursement of State Unemployment Benefits at Height of Pandemic." Consumer Financial Protection Bureau, July 14, 2022. https://www.consumerfinance.gov/about-us/newsroom/federal-regulators-fine-bank-of-america-225-million-over-botched-disbursement-of-state-unemployment-benefits-at-height-of-pandemic/.

———. "Helping Consumers Who Have Been Denied Checking Accounts." Consumer Financial Protection Bureau, 2016. https://files.consumerfinance.gov/f/201602_cfpb_helping-consumers-who-have-been-denied-checking-accounts.pdf.

———. "Required Rulemaking on Personal Financial Data Rights." *Federal Register*, October 31, 2023. https://www.federalregister.gov/d/2023-23576.

———. "Small Business Advisory Review Panel for Consumer Reporting Rulemaking: Outline of Proposals and Alternatives Under Consideration." Consumer Financial Protection Bureau, September 15, 2023. https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf.

Consumerist. "TransUnion Must Pay $60M For Mistakenly Tagging People As Possible Terrorists." Consumer Reports, March 8, 2018. https://www.consumerreports.org/consumerist/transunion-must-pay-60m-for-mistakenly-tagging-people-as-possible-terrorists/.

Cox, Joseph. "An Instant Fake ID Factory." 404 Media, February 5, 2024. https://www.404media.co/email/7ba8cca7-96d2-487d-a1e3-5cc0de98fc4e/.

Crossman, Penny. "Rushed Anti-Money-Laundering Calls Backfire. Can AI Help?" *American Banker*, December 4, 2023. https://www.americanbanker.com/news/rushed-anti-money-laundering-calls-backfire-can-ai-help.

Cruz, Brett. "52 Million Americans Experienced Credit Card Fraud Last Year." *Security.Org* (blog). Accessed September 30, 2024. https://www.security.org/digital-safety/credit-card-fraud-report/.

Dayen, David. "USPS Begins Postal Banking Pilot Program." The American Prospect, October 4, 2021. https://prospect.org/api/content/55664c28-24a9-11ec-84ba-12f1225286c6/.

DeLiema, Marguerite, Gary Mottola, and Martha Deevy. "Findings from a Pilot Study to Measure Financial Fraud in the United States." Stanford Center on Longevity, February 2017. https://longevity.stanford.edu/financial-fraud-research-center/wp-content/uploads/2017/02/SCL-Fraud-Report-Feb-2017_Draft2.pdf.

DeLiema, Marguerite, and Paul Witt. "Profiling Consumers Who Reported Mass Marketing Scams: Demographic Characteristics and Emotional Sentiments Associated with Victimization." *Security Journal* 37, no. 3 (September 1, 2024): 921–64. https://doi.org/10.1057/s41284-023-00401-5.

DeLiema, Marti, Emma Fletcher, Christine N. Kieffer, Gary R. Mottola, Rubens Pessanha, and Melissa Trumpower. "Exposed to Scams: What Separates Victims from Non-Victims?" Stanford Center on Longevity, September 2019. https://longevity.stanford.edu/wp-content/uploads/2019/09/ScamTrackerIssueBrief-ExposedToScamsReducedFile.pdf.

Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, and Saniya Ansar. "The Global Findex Database 2021." The World Bank Group, 2022. https://www.worldbank.org/en/publication/globalfindex/Report.

Dilanian, Ken, Kit Ramgopal, and Chloe Atkins. "'Easy Money': How International Scam Artists Pulled off an Epic Theft of Covid Benefits." NBC News, August 15, 2021. https://www.nbcnews.com/news/us-news/easy-money-how-international-scam-artists-pulled-epic-theft-covid-n1276789.

Dock. "Zero-Knowledge Proofs: Non-Techie's Guide to Online Privacy Tech." Dock.io, October 2, 2024. https://www.dock.io/post/zero-knowledge-proofs.

Doubleday, Justin. "SSA Built a System to Help Combat Identity Fraud. Backers Say It's 'at Risk of Collapse.'" *Federal News Network*, June 30, 2023. https://federalnewsnetwork.com/management/2023/06/ssa-built-a-system-to-help-combat-identity-fraud-backers-say-its-at-risk-of-collapse/.

Eckerle, Patrick. "When Failing an eCBSV Verification Isn't Indicative of Risk." *Sentilink* (blog), June 9, 2023. https://resources.sentilink.com/blog/an-analysis-of-ecbsv-mismatches.

Ellen Segal Huvelle. Individual Reference Services Group, Inc. and TransUnion LLC v. Federal Trade Commission, et al. (United States District Court for the District of Columbia April 30, 2001).

European Commission. "Building Trust in Human Centric Artificial Intelligence." European Commission, April 8, 2019. https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence.

———. "Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence." European Commission, April 21, 2021. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

European Parliament. "Artificial Intelligence Act." European Parliament, 2023. https://artificialintelligenceact.eu/the-act/.

Faceplugin. "Active Liveness Detection vs Passive Liveness Detection." *Medium* (blog), April 29, 2024. https://medium.com/@faceplugin/active-liveness-detection-vs-passive-liveness-detection-0477818695ca.

Faz, Xavier. "Mexico's Tiered KYC: An Update on Market Response." *CGAP* (blog), June 25, 2013. https://www.cgap.org/blog/mexicos-tiered-kyc-update-on-market-response, https://www.cgap.org/blog/mexicos-tiered-kyc-update-on-market-response.

Federal Bureau of Investigation Internet Crime Complaint Center. "Elder Fraud Report 2023." Federal Bureau of Investigation Internet Crime Complaint Center, December 12, 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf.

Federal Deposit Insurance Corporation. "Connecting the Dots…The Importance of Timely and Effective Suspicious Activity Reports." *FDIC Supervisory Insights*, 2007. https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/siwinter2007-article03.html.

Federal Financial Institutions Examination Council. "BSA/AML Manual / Assessing Compliance with BSA Regulatory Requirements / Currency Transaction Reporting." Federal Financial Institutions Examination Council BSA/AML InfoBase. Accessed August 12, 2024. https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/05.

———. "BSA/AML Manual / Office of Foreign Assets Control." Federal Financial Institutions Examination Council BSA/AML InfoBase. Accessed August 12, 2024. https://bsaaml.ffiec.gov/manual/OfficeOfForeignAssetsControl/01.

Federal Register. “Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Extending Enforcement Date.” March 9, 2023. https://www.federalregister.gov/d/2023-04496.

Federal Trade Commission. “Consumer Sentinel Network: Data Book 2022.” Federal Trade Commission, February 2023.

———. “Data Brokers: A Call for Transparency and Accountability,” May 2014. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

———. “Fraud Reports.” Accessed August 13, 2024. https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses.

Financial Crimes Enforcement Network. “Answers to Frequently Asked Bank Secrecy Act (BSA) Questions.” FinCEN.gov. Accessed October 2, 2024. https://www.fincen.gov/answers-frequently-asked-bank-secrecy-act-bsa-questions.

———. “Customer Due Diligence Requirements for Financial Institutions: Final Rules.” *The Federal Register*, May 11, 2016. https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

———. “FinCEN Assesses Record $1.3 Billion Penalty against TD Bank.” FinCEN.gov, October 10, 2024. https://www.fincen.gov/news/news-releases/fincen-assesses-record-13-billion-penalty-against-td-bank.

———. “FinCEN Suspicious Activity Report Electronic Filing Requirements Version 1.4.” Financial Crimes Enforcement Network, March 2015. https://bsaefiling.fincen.treas.gov/docs/FinCENSARElectronicFilingRequirements.pdf.

———. “Funds ‘Travel’ Regulations: Questions & Answers.” *FinCEN Advisory*, January 1997.

———. “SAR Stats.” Financial Crimes Enforcement Network, July 31, 2024. https://www.fincen.gov/reports/sar-stats.

———. “Section 314(b) Fact Sheet.” Financial Crimes Enforcement Network, December 2020. https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

“Financial Crimes Enforcement Network (FinCEN) Year in Review for FY 2023.” Financial Crimes Enforcement Network, June 7, 2024. https://www.fincen.gov/sites/default/files/shared/FinCEN_Infographic_Public_508FINAL_2024_June_7.pdf.

Fines and Fees Justice Center. “Free to Drive: End Driver’s License Suspensions for Unpaid Fines and Fees.” *Fines and Fees Justice Center* (blog). Accessed October 2, 2024. https://finesandfeesjusticecenter.org/campaigns/national-drivers-license-suspension-campaign-free-to-drive/.

Finicity. “Instant Bank Account Verification | Account Owner Validation.” *Finicity* (blog). Accessed September 18, 2024. https://www.finicity.com/pay/ach-account-owner/.

FinRegLab. “Assessing Federated Machine Learning’s Potential for Transforming KYC/AML.” FinRegLab, November 2020. https://finreglab.org/wp-content/uploads/2023/12/FinRegLab_2020-11-03_Proposed-Research_Assessing-Federated-Learning-for-BSA-AML.pdf.

———. “Explainability & Fairness in Machine Learning for Credit Underwriting: Policy & Empirical Findings Overview.” FinRegLab, July 2023. https://finreglab.org/research/explainability-fairness-in-machine-learning-for-credit-underwriting-policy-empirical-findings-overview/.

———. “Explainability & Fairness in Machine Learning for Credit Underwriting: Policy Analysis.” FinRegLab, December 2023. https://finreglab.org/research/explainability-fairness-in-machine-learning-for-credit-underwriting-policy-analysis/.

———. “Machine Learning Explainability & Fairness: Insights from Consumer Lending.” FinRegLab, July 2023. https://finreglab.org/research/machine-learning-explainability-fairness-insights-from-consumer-lending/.

Fisher, Bill. “Check Your Wallet? How Mobile Driver’s Licenses Are Changing Online Transactions.” *NIST*, May 22, 2024. https://www.nist.gov/blogs/cybersecurity-insights/check-your-wallet-how-mobile-drivers-licenses-are-changing-online.

Fitzgerald, Kate. “Inside FIS’ Use of AI to Weed out False-Positive Card Fraud Alerts.” *American Banker*, April 16, 2024. https://www.americanbanker.com/payments/news/inside-fis-use-of-ai-to-weed-out-false-positive-card-fraud-alerts.

FRB Services. “Fraud and Instant Payments: The Basics.” FRBservices.org. Accessed August 13, 2024. https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html.

Gacki, Andrea. “Prepared Remarks for the Identity Project Colloquium in Washington, DC,” June 17, 2024. https://www.fincen.gov/sites/default/files/2024-06/PREPARED-REMARKS-IDENTITY-PROJECT-COLLOQUIUM-FINAL-508_0.pdf.

Galluzzo, Ryan, Connie LaSalle, Maria Vachino, and Richard Newbold. “Attribute Validation Services for Identity Management: Architecture, Security, Privacy, and Operational Considerations.” NIST Interagency Report. National Institute of Standards and Technology, October 2024. https://doi.org/10.6028/NIST.IR.8480.ipd.

Gegory, Aaron M. “FinCEN: Docket Number FINCEN-2020-0002; RIN 1506-AB41 Board: Docket Number R-1726; RIN 7100-AF97,” November 27, 2020. https://www.federalreserve.gov/SECRS/2020/December/20201222/R-1726/R-1726_112520_137397_442005400994_1.pdf.

“Getting to Effectiveness - Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance.” Bank Policy Institute, October 29, 2018. https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf.

Hanmer, Michael J., and Samuel B. Novey. “Who Lacked Photo ID in 2020?: An Exploration of the American National Election Studies.” University of Maryland Center for Democracy and Civic Engagement, March 13, 2023.

Hanoch, Yaniv, and Stacey Wood. “The Scams Among Us: Who Falls Prey and Why.” *Current Directions in Psychological Science* 30, no. 3 (June 1, 2021): 260–66. https://doi.org/10.1177/0963721421995489.

Heinbuch, Scarlett. "Overcoming KYC Banking Barriers: A Lesson from Mexico." *Take on Payments from the Federal Reserve Bank of Atlanta* (blog), January 8, 2024. https://www.atlantafed.org/blogs/take-on-payments/2024/01/08/overcoming-kyc-banking-barriers--lesson-from-mexico.

HM Treasury. "The Payment Services (Amendment) Regulations 2024: Policy Note." HM Treasury, March 2024. https://assets.publishing.service.gov.uk/media/65eed7233649a26deded630f/Policy_note.pdf.

Horan, TJ. "Real-Time Payments Fraud Is Growing - Here's How to Prevent It." *FICO Blog* (blog), October 17, 2023. https://www.fico.com/blogs/real-time-payments-fraud-growing-heres-how-prevent-it.

IBM Research. "What Is Federated Learning?" IBM Research, February 9, 2021. https://research.ibm.com/blog/what-is-federated-learning.

IDcentral. "Tiered KYC in Indian Payment Banks: Boosting Financial Inclusion." *IDcentral* (blog), February 9, 2024. https://www.idcentral.io/blog/tiered-kyc-in-indian-payment-banks-boosting-financial-inclusion/.

Identity Theft Resource Center. "Identity in Practice Report: Understanding Identity Crimes in Black Communities." Identity Theft Resource Center, September 2023. https://www.idtheftcenter.org/publication/identity-in-practice-report/.

"Identity-Related Suspicious Activity: 2021 Threats and Trends." Financial Trend Analysis. Financial Crimes Enforcement Network, January 2024.

IDNYC. "Banks & Credit Unions - IDNYC." Accessed August 12, 2024. https://www.nyc.gov/site/idnyc/benefits/banks-and-credit-unions.page.

IDNYC. "Document Calculator - How to Apply - IDNYC." Accessed August 12, 2024. https://www.nyc.gov/site/idnyc/card/documentation.page.

Internal Revenue Service. "Acceptable Documents to Submit Your ITIN Application." Internal Revenue Service, January 4, 2024. https://www.irs.gov/forms-pubs/acceptable-documents-to-submit-your-itin-application.

———. "Instructions for Form W-7." Internal Revenue Service, November 2023.

ISO. "ISO/IEC TS 18013-7: Life Cycle," September 18, 2024. https://www.iso.org/standard/82772.html.

ISO20022. "About ISO 20022." Accessed August 13, 2024. https://www.iso20022.org/about-iso-20022.

"ISO/IEC 18013-5:2021." International Organization for Standardization, September 2021. https://www.iso.org/standard/69084.html.

ITRC. "Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High." Accessed August 2, 2024. https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/.

Javelin Research. "Overcoming False Positive Declines in E-Commerce." Javelin Research, December 2018. https://nudatasecurity.com/wp-content/uploads/2019/01/Javelin-Report-for-NuData-Overcoming-False-Positive-Declines-in-E-Commerce-NuData-Security.pdf.

Jeník, Ivo, Mehmet Kerse, and Louis De Koker. "FATF's Proposed Rules for Payments: Balancing Integrity and Inclusion?" *CGAP* (blog), May 1, 2024. https://www.cgap.org/blog/fatfs-proposed-rules-for-payments-balancing-integrity-and-inclusion, https://www.cgap.org/blog/fatfs-proposed-rules-for-payments-balancing-integrity-and-inclusion.

Jensen, Rasmus Ingemann Tuffveson, Joras Ferwerda, Kristian Sand Jørgensen, Erik Rathje Jensen, Martin Borg, Morten Persson Krogh, Jonas Brunholm Jensen, and Alexandros Iosifidis. "A Synthetic Data Set to Benchmark Anti-Money Laundering Methods." *Scientific Data* 10, no. 1 (September 28, 2023): 661. https://doi.org/10.1038/s41597-023-02569-2.

Jeydel, Steptoe LLP-Peter Edward, Jack R. Hayes, and Brian Egan. "OFAC Asserts Jurisdiction over French Banks's Internal Transfers and Foreign Exchange Transactions." *Lexology International Compliance Blog* (blog), January 15, 2021. https://www.lexology.com/library/detail.aspx?g=2d8f38b0-4ad3-4622-a1ca-78dfcd6d0b08.

Jingnan, Huo. "Using AI to Detect AI-Generated Deepfakes Can Work for Audio — but Not Always." *NPR*, April 5, 2024, sec. Untangling Disinformation. https://www.npr.org/2024/04/05/1241446778/deepfake-audio-detection.

Johnson, Aurora, and Mike Dausin. "What to Know About the National Public Data Breach—Is It Worthy of the Hype?" *SpyCloud* (blog), August 22, 2024. https://spycloud.com/blog/national-public-data-breach-analysis/.

Karkal, Shamir. "How to Fight Growing ACH Fraud." *Bank Automation News* (blog), February 24, 2023. https://bankautomationnews.com/allposts/risk-security/how-to-fight-growing-ach-fraud/, https://bankautomationnews.com/allposts/risk-security/how-to-fight-growing-ach-fraud/.

Kessler, Carson. "A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money." ProPublica, July 6, 2021. https://www.propublica.org/article/chime.

Ketenci, Utku Görkem, Tolga Kurt, Selim Önal, Cenk Erbil, Sinan Aktürkoğlu, and Hande Şerban İlhan. "A Time-Frequency Based Suspicious Activity Detection for Anti-Money Laundering." *IEEE Access* 9 (2021): 59957–67. https://doi.org/10.1109/ACCESS.2021.3072114.

Klar, Rebecca. "Data Privacy Bill Markup Canceled after House Leadership Opposition." Text. *The Hill* (blog), June 27, 2024. https://thehill.com/homenews/house/4742987-data-privacy-bill-markup-cancelled-after-house-leadership-opposition/.

Koker, Louis De. "Editorial: Regulatory Impact Assessment: Towards a Better Approach for the FATF." *Journal of Money Laundering Control* 25, no. 2 (2022): 265–67. http://dx.doi.org/10.1108/JMLC-05-2022-149.

KPMG. "Fighting Fraud with a Model of Models." KPMG, 2020. https://assets.kpmg.com/content/dam/kpmg/dk/pdf/dk-2020/04/Nets-KPMG-Fighting-Fraud-with-a-Model-of-Models-whitepaper-2020.pdf.

Krajewska, Magdalena. "Implementing the REAL ID Act: Intergovernmental Conflict and Cooperation in Homeland Security Policy." *Publius: The Journal of Federalism* 50, no. 3 (July 1, 2020): 398–422. https://doi.org/10.1093/publius/pjaa010.

Land, Jennifer. "Lone Star Credit Union Successfully Pilots New BonifiID Identity Credential from Bonifii and GlobaliD." Bonifii, September 11, 2023. https://bonifii.com/2023/09/lone-star-credit-union-successfully-pilots-new-bonifiid-identity-credential-from-bonifii-and-globalid/.

Lasisi, Sodiq. "The Thrilling World of Tiered KYC in Nigeria (Designer Edition)." *Medium* (blog), December 3, 2023. https://sodiqlasisi.medium.com/the-need-for-trust-and-security-has-never-been-more-paramount-5ef173393a04.

Leffer, Lauren. "AI Audio Deepfakes Are Quickly Outpacing Detection." Scientific American. Accessed August 2, 2024. https://www.scientificamerican.com/article/ai-audio-deepfakes-are-quickly-outpacing-detection/.

Leisure, Mindy. "ITIN's—What You Need to Know." *Advantage Credit* (blog), June 27, 2024. https://www.advcredit.com/itins/.

"Leveraging Generative AI (GenAI) for Fraud Detection and Prevention." Accessed August 2, 2024. https://www.turing.com/resources/generative-ai-fraud-detection.

LexisNexis. "True Cost of Financial Crime Compliance Study 2023: U.S. & Canada." LexisNexis, 2024. https://risk.lexisnexis.com/insights-resources/research/true-cost-of-financial-crime-compliance-study-for-the-united-states-and-canada.

Lieber, Ron, and Tara Siegel Bernard. "Why Banks Are Suddenly Closing Down Customer Accounts." *The New York Times*, November 5, 2023, sec. Business. https://www.nytimes.com/2023/11/05/business/banks-accounts-close-suddenly.html.

Lord, Nate. "What Is Public Key Cryptography? (And How It Works)." Text. *DataInsider, Digital Guardian's Blog* (blog), May 6, 2023. https://www.digitalguardian.com/blog/what-public-key-cryptography.

Lovett, Kenneth. "New York State Wants Banks to Accept City Municipal ID Cards to Help Immigrants Wishing to Open an Account." *New York Daily News*, April 8, 2018. https://www.nydailynews.com/2016/09/05/exclusive-new-york-state-wants-banks-to-accept-city-municipal-id-cards-to-help-immigrants-wishing-to-open-an-account/.

Ludwig, Heiko, and Nathalie Baracaldo, eds. "Federated Learning: A Comprehensive Overview of Methods and Applications." In *Federated Learning: A Comprehensive Overview of Methods and Applications*, 337–61. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-96896-0_15.

Lumley, Liz. "US Real-Time Payments Are in Their Early Days, but Show Steady Growth." *The Banker*, May 2022. https://www.thebanker.com/US-real-time-payments-are-in-their-early-days-but-show-steady-growth-1716362818.

Magramo, Kathleen. "Gangs Netting up to $3 Trillion a Year as Southeast Asia Human Trafficking Becomes a Global Crisis, Interpol Says." CNN, March 28, 2024. https://www.cnn.com/2024/03/28/asia/southeast-asia-interpol-scam-human-trafficking-crime-intl-hnk/index.html.

McCaffrey, Orla. "ABA to Launch Information-Sharing Exchange to Help Banks Fight Fraud." *American Banker*, November 29, 2023. https://www.americanbanker.com/news/aba-to-launch-information-sharing-exchange-to-help-banks-fight-fraud.

McDonald, Owen. "Check Fraud Is Up Nearly 400% and FinCEN Points to Banks." Bottomline, September 24, 2024. https://www.bottomline.com/resources/blog/check-fraud-is-up-nearly-400-and-fincen-points-to-banks.

McGreevy, Patrick. "Bank of America Must Provide More Proof of Fraud before Freezing EDD Accounts, Court Orders." *Los Angeles Times*, June 1, 2021, sec. California. https://www.latimes.com/california/story/2021-06-01/bank-of-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california.

Medintz, Scott. "Black and Latino Consumers Are More Likely to Lose Money to Digital Scams, a Consumer Reports Study Finds." Consumer Reports, October 1, 2024. https://www.consumerreports.org/money/scams-fraud/black-latino-consumers-more-likely-to-lose-money-in-scams-a7652153980/.

Moody's. "From KYC to KYB: The Key Differences and Best Practices." *Moody's* (blog), September 16, 2022. https://www.moodys.com/web/en/us/kyc/resources/insights/kyc-kyb-key-differences-best-practices.html.

Morgan, Rachel E. "Financial Fraud in the United States, 2017." U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, April 2021.

Morgan, Rachel E., and Susannah N. Tapp. "Examining Financial Fraud Against Older Adults." National Institute of Justice, March 20, 2024. https://nij.ojp.gov/topics/articles/examining-financial-fraud-against-older-adults.

Morris, Chris. "The Number of Data Breach Victims Is up 490% in the First Half of 2024." Fast Company, July 18, 2024. https://www.fastcompany.com/91158122/data-breach-victims-up-490-percent-first-half-2024.

Movement Advancement Project. "The ID Divide: How Barriers to ID Impact Different Communities and Affect Us All." Movement Advancement Project, November 2022. https://www.mapresearch.org/file/MAP-Identity-Documents-report-2022.pdf.

MX. "Secure, Instant Identity and Account Verifications." MX. Accessed September 18, 2024. https://mx.com.

Nasdaq Verafin. "Global Financial Crime Report: Insights at the Intersection of Financial Crime Data & Real Survivor Rates." Nasdaq Verafin, 2024.

National Conference of State Legislatures. "States Offering Driver's Licenses to Immigrants." National Conference of State Legislatures, March 13, 2023. https://www.ncsl.org/immigration/states-offering-drivers-licenses-to-immigrants.

National Consumer Law Center. "Letter from Coalition of Immigrant, Consumer, and Privacy Groups Urging CFPB to Use FCRA to Rein in Data Brokers." NCLC, February 8, 2023. https://www.nclc.org/resources/letter-from-coalition-of-immigrant-consumer-and-privacy-groups-urging-cfpb-to-use-fcra-to-rein-in-data-brokers/.

National Institute of Standards and Technology. "Accelerating the Adoption of Mobile Driver's Licenses." National Institute of Standards and Technology, May 2024. https://www.nccoe.nist.gov/sites/default/files/2024-05/mdl-fact-sheet.pdf.

National Iranian American Council. "Memo: Ending Discriminatory Bank Account Closures," July 21, 2022. https://www.niacouncil.org/news_publications/memo-ending-discriminatory-bank-account-closures/.

NIST NCCoE. "NCCoE Announces Collaborators | Mobile Driver's License (mDL) Project Use Case #1." NIST NCCoE, August 20, 2024. https://www.nccoe.nist.gov/news-insights/nccoe-announces-collaborators-mobile-drivers-license-mdl-project-use-case-1.

"NIST SP 800-63 Digital Identity Guidelines," 2020. https://pages.nist.gov/.

NIST.gov. "Digital Identities - mDL | NCCoE." Accessed August 19, 2024. https://www.nccoe.nist.gov/projects/digital-identities-mdl.

NYC Consumer and Worker Protection. "IDNYC Banking Access Campaign." Accessed August 6, 2024. https://www.nyc.gov/site/dca/media/idnyc-savings-account.page.

Office of Foreign Assets Control. "Additional Questions from Financial Institutions." Office of Foreign Assets Control, 2002. https://ofac.treasury.gov/faqs/topic/1621.

Office of the Comptroller of the Currency. "Can the Bank Close My Checking Account and Not Notify Me?" HelpWithMyBank.gov, April 2021. https://www.helpwithmybank.gov/help-topics/bank-accounts/opening-closing-inactive-bank-accounts/closing-a-bank-account/closing-notification.html.

Ostmann, Florian, and Cosmina Dorobantu. "AI in Financial Services." The Alan Turing Institute, n.d. https://doi.org/10.5281/zenodo.4916041.

Oztas, Berkan, Deniz Cetinkaya, Festus Adedoyin, Marcin Budka, Gokhan Aksu, and Huseyin Dogan. "Transaction Monitoring in Anti-Money Laundering: A Qualitative Analysis and Points of View from Industry." *Future Generation Computer Systems* 159 (October 1, 2024): 161–71. https://doi.org/10.1016/j.future.2024.05.027.

Pape, Carter. "Sharing Fraud Data Is Hard. Two Industry Efforts Aim to Make It Easier." *American Banker*, April 24, 2024. https://www.americanbanker.com/news/sharing-fraud-data-is-hard-two-industry-efforts-aim-to-make-it-easier.

———. "Treasury Accuses Banks of 'insufficient Data Sharing' on Fraud." *American Banker*, April 2, 2024. https://www.americanbanker.com/news/treasury-accuses-banks-of-insufficient-data-sharing-on-fraud.

Pol, Ronald F. "Anti-Money Laundering: The World's Least Effective Policy Experiment? Together, We Can Fix It." *Policy Design and Practice* 3, no. 1 (January 2, 2020): 73–94. https://doi.org/10.1080/25741292.2020.1725366.

"Project Aurora: The Power of Data, Technology, and Collaboration to Combat Money Laundering across Institutions and Borders." The Bank for International Settlements' Innovation Hub, May 2023. https://www.bis.org/publ/othp66.pdf.

PYMNTS. "A False Declined Payment Costs Merchants More Than a Sale." *PYMNTS.Com* (blog), December 18, 2023. https://www.pymnts.com/news/ecommerce/2023/false-declined-payment-costs-merchants-more-than-sale/.

———. "Deep Dive: How Merchants Can Reduce the Risk of False Positives Through AI and ML." *PYMNTS.Com* (blog), September 10, 2021. https://www.pymnts.com/fraud-prevention/2021/deep-dive-merchants-reduce-risk-false-positives-artificial-intelligence-machine-learning/.

———. "Digital Wallets Exhibit Highest Increase in Fraud Among All Payment Methods." *PYMNTS.Com* (blog), October 20, 2023. https://www.pymnts.com/fraud-prevention/2023/digital-wallets-exhibit-highest-increase-in-fraud-among-all-payment-methods/.

———. "Jack Henry Debuts Defense Against Money Laundering." *PYMNTS.Com* (blog), October 16, 2023. https://www.pymnts.com/aml/2023/jack-henry-debuts-defense-against-money-laundering/.

———. "Nearly 60% of Firms Say Failed Payments Are Expensive to Track and Resolve." *PYMNTS.Com* (blog), February 23, 2024. https://www.pymnts.com/digital-payments/2024/nearly-60-of-firms-say-failed-payments-are-expensive-to-track-and-resolve/.

Qi, Hua, Qing Guo, Felix Juefei-Xu, Xiaofei Xie, Lei Ma, Wei Feng, Yang Liu, and Jianjun Zhao. "DeepRhythm: Exposing DeepFakes with Attentional Visual Heartbeat Rhythms." arXiv, August 26, 2020. https://doi.org/10.48550/arXiv.2006.07634.

Rothschild, Jillian Andres, Samuel B. Novey, and Michael J. Hanmer. "Who Lacks ID in America Today? An Exploration of Voter ID Access, Barriers, and Knowledge." University of Maryland Center for Democracy and Civic Engagement, June 2024. https://cdce.umd.edu/sites/cdce.umd.edu/files/pubs/Voter%20ID%20survey%20Key%20Results%20June%202024.pdf.

San Francisco Office of Financial Empowerment. "Blacklisted: How ChexSystems Contributes to Systemic Financial Exclusion." San Francisco Office of Financial Empowerment, June 2021. https://www.sfgov.org/ofe/sites/default/files/2021-06/Blacklisted-How%20ChexSystems%20Contributes%20to%20Systematic%20Financial%20Exclusions%20-%20FINAL.pdf.

Sanchez-Adams, Carla. "Testimony before the U.S. Senate Committee on Banking, Housing, and Urban Affairs: Examining Scams and Fraud in the Banking System and Their Impact on Consumers." National Consumer Law Center, February 1, 2024. https://www.nclc.org/wp-content/uploads/2024/02/Written-testimony-The-Problem-of-Payment-Fraud.pdf.

Sen, Jaydip, Hetvi Waghela, and Sneha Rakshit. "Privacy in Federated Learning." arXiv, August 12, 2024. https://doi.org/10.48550/arXiv.2408.08904.

"Serving Communities of Color: A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color." Federal Trade COmmission, October 2021.

Sharma, Amit, and Sena Lloyd. "Empowering Constituents through Web3: A Vision for Personal Financial Data Rights." *Fintech Today* (blog), May 14, 2024. https://financialtechnologytoday.com/empowering-constituents-through-web3-a-vision-for-personal-financial-data-rights/.

Shelley Thompson. "Re: Forthcoming CFPB 'Data Broker' Rulemaking under the FCRA." Consumer Bankers Association, September 5, 2023. https://consumerbankers.com/wp-content/uploads/2024/03/CBA-Credit-Header-Data-Letter-to-CFPB_FINAL.pdf.

Shepherd, Kevin L., Alexander W. Koff, and Michael D. Schiffer. "Looming Reporting Deadline Under the Corporate Transparency Act: The Reality Sets In." Venable LLP. Accessed October 2, 2024. https://www.venable.com/insights/publications/2024/09/looming-reporting-deadline-under-the-corporate.

Shoemaker, Phillip. "Verifiable Credentials: The Future of Digital Identity." *Identity* (blog), September 25, 2024. https://www.identity.com/what-are-verifiable-credentials/.

Smethurst, Reilly. "Digital Identity Wallets and Their Semantic Contradictions." *ECIS 2023 Research Papers*, May 11, 2023. https://aisel.aisnet.org/ecis2023_rp/288.

Sovrin. "What Is Self-Sovereign Identity?" *Sovrin* (blog). Accessed August 19, 2024. https://sovrin.org/faq/what-is-self-sovereign-identity/.

Spiotto, Ann H. "Credit, Debit, or ACH: Consequences & Liabilities A Comparison of the Differences in Consumer Liabilities." Emerging Payments Occasional Paper Series. Federal Reserve Bank of Chicago, September 2001. https://www.chicagofed.org/-/media/others/research/papers/payments-studies-occasional-papers-series/eps-2001-3-pdf.pdf.

Sporny, Manu, Dave Longley, David Chadwick, and Orie Steele. "Verifiable Credentials Data Model v2.0." World Wide Web Consortium, September 26, 2024. https://www.w3.org/TR/vc-data-model-2.0/.

Stanton, Brian, and Theodore Jensen. "Trust and Artificial Intelligence (Draft)." NIST, March 2, 2021. https://www.nist.gov/publications/trust-and-artificial-intelligence-draft.

"Synthetic Data Generation: Definition, Types, Techniques, & Tools." Accessed August 2, 2024. https://www.turing.com/kb/synthetic-data-generation-techniques.

Taxpayer Advocate Service. "Reducing 'False Positive' Determinations in Fraud Detection." *Taxpayer Advocate Service - 2016 Annual Report to Congress* 3 (2016). https://www.taxpayeradvocate.irs.gov/wp-content/uploads/2020/08/ARC16_Volume3_07_ReducingFalsePositive.pdf.

The Aspen Institute. "Aspen FSP Launches National Task Force for Fraud & Scam Prevention," July 18, 2024. https://www.aspeninstitute.org/blog-posts/aspen-fsp-launches-national-task-force-for-fraud-scam-prevention/.

The Bank for International Settlements. "Report to the G20: Harmonised ISO 20022 Data Requirements for Enhancing Cross-Border Payments." The Bank for International Settlements' Committee on Payments and Market Infrastructures, October 2023. https://www.bis.org/cpmi/publ/d218.pdf.

The Better Identity Coalition. "Better Identity in America: A Blueprint for Policymakers." The Better Identity Coalition, July 2018. https://sccitp.senate.ca.gov/sites/sccitp.senate.ca.gov/files/Better_Identity_Coalition%20Blueprint%20-%20July%202018.pdf.

"The Department of the Treasury's De-Risking Strategy." U.S. Department of the Treasury, April 2023. https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf.

"The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation." The Financial Action Task Force, November 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf.

The Federal Trade Commission. "Protecting Older Consumers 2022-2023." The Federal Trade Commission, October 2023. https://www.ftc.gov/reports/protecting-older-consumers-2022-2023-report-federal-trade-commission.

The Financial Action Task Force. "Countries." The Financial Action Task Force. Accessed August 13, 2024. https://www.fatf-gafi.org/en/countries.html.

———. "Guidance on Digital ID." The Financial Action Task Force, March 6, 2020. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html.

———. "High-Risk and Other Monitored Jurisdictions." The Financial Action Task Force. Accessed August 13, 2024. https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html.

———. "Public Consultation on Recommendation 16 on Payment Transparency." The Financial Action Task Force, February 26, 2024. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R16-public-consultation-Feb24.html.

———. "United States: 7th Follow-Up Report & Technical Compliance Re-Rating." The Financial Action Task Force, March 2024. https://www.fatf-gafi.org/content/dam/fatf-gafi/fur/USA-FUR-2024.pdf.coredownload.inline.pdf.

The World Bank Group. "De-Risking in the Financial Sector." Text/HTML. World Bank, October 7, 2016. https://www.worldbank.org/en/topic/financialsector/brief/de-risking-in-the-financial-sector.

———. "ID4D and G2Px 2022 Annual Report." The World Bank Group, 2023. https://documents1.worldbank.org/curated/en/099437402012317995/pdf/IDU00fd54093061a70475b0a3b50dd7e6cdfe147.pdf.

———. "Volume 1: Global ID Coverage Estimates." ID4D Global Dataset 2021. The World Bank Group, 2022. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099705012232226786/p176341132c1ef0b21adf11abad304425ef.

Timoney, Mike. "Why Is Check Fraud Suddenly Rampant?" Federal Reserve Bank of Boston, August 23, 2023. https://www.bostonfed.org/news-and-events/news/2023/08/check-fraud-rampant-mike-timoney-column-fraud-awareness-key-to-slowing-surge.aspx.

T.J. Horan. "Evolution of Fraud Analytics - An Inside Story." *KDnuggets* (blog), March 14, 2014. https://www.kdnuggets.com/evolution-of-fraud-analytics-an-inside-story.

TransUnion. "TransUnion Analysis Finds Synthetic Identity Fraud Growing to Record Levels," August 24, 2023. https://newsroom.transunion.com/transunion-analysis-finds-synthetic-identity-fraud-growing-to-record-levels/.

Treasury Inspector General for Tax Administration. "Administration of the Individual Taxpayer Identification Number Program." Treasury Inspector General for Tax Administration, December 19, 2023.

Trew, Heather. "Closing the Book on Account Closures." *ABA Banking Journal*, January 22, 2024. https://bankingjournal.aba.com/2024/01/closing-the-book-on-account-closures/.

U. S. Government Accountability Office. "Anti-Money Laundering: Better Information Needed on Effectiveness of Federal Efforts." U.S. Government Accountability Office, June 13, 2024. https://www.gao.gov/products/gao-24-106301.

United Nations : Office on Drugs and Crime. "Money Laundering Overview." Accessed August 2, 2024. https://www.unodc.org/unodc/en/money-laundering/overview.html.

United States Committee on Banking, Housing, and Urban Affairs. "Brown Presses Banks on Voice Authentication Services." United States Committee on Banking, Housing, and Urban Affairs, May 4, 2023. https://www.banking.senate.gov/newsroom/majority/brown-presses-banks-voice-authentication-services.

United States Department of Justice. "U.S. Department of Transportation Takes Action to Ensure Equitable Driver License Office Access for Alabama Residents," December 28, 2016.

United States Department of Justice Office of Public Affairs. "Press Release: Justice Department Announces Results of Nationwide COVID-19 Fraud Enforcement Action," August 23, 2023. https://www.justice.gov/opa/pr/justice-department-announces-results-nationwide-covid-19-fraud-enforcement-action.

United States Department of State. "De-Risking." *United States Department of State* (blog). Accessed August 13, 2024. https://www.state.gov/de-risking/.

US Birth Certificates. "Why Laminating Your Birth Certificate Is Not a Good Idea," May 27, 2021.

U.S. Department of the Treasury. "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector." U.S. Department of the Treasury, March 2024. https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf.

———. "Press Release: Final Rule for Electronic Government Payments Will Balance Recipient Needs with Benefits of Electronic Payment." U.S. Department of the Treasury, June 25, 1998. https://home.treasury.gov/news/press-releases/rr2560.

U.S. Government Accountability Office. "Payment Scams: Information on Financial Industry Efforts." U.S. Government Accountability Office, July 25, 2024. https://www.gao.gov/assets/880/870111.pdf.

Vittorio, Andrea, and Evan Weinberger. "Sales of Personal Data on Consumer Credit Reports Draw Scrutiny." *Bloomberg Law*, August 17, 2023. https://news.bloomberglaw.com/privacy-and-data-security/sales-of-personal-data-on-consumer-credit-reports-draw-scrutiny.

Vorobyev, Ivan, and Anna Krivitskaya. "Reducing False Positives in Bank Anti-Fraud Systems Based on Rule Induction in Distributed Tree-Based Models." *Computers & Security* 120 (September 1, 2022): 102786. https://doi.org/10.1016/j.cose.2022.102786.

Wang, Kailai. "Are Generation Z Less Car-Centric Than Millennials? A Nationwide Analysis Through the Lens of Youth Licensing." *Cities* 149 (June 1, 2024): 104951. https://doi.org/10.1016/j.cities.2024.104951.

Wei, Joannie, Rosario Mendez, Kati Daffan, Patti Poss, and Rhonda Perkins. "Serving Communities of Color." Federal Trade Commission, 2021. https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf.

Whelehan, Barbara. "What Is ChexSystems?" Bankrate, December 19, 2023. https://www.bankrate.com/banking/checking/what-is-chexsystems/.

White, Olivia, Anu Madgavkar, James Manyika, Deepa Mahajan, Jacques Bughin, Michael McCarthy, and Owen Sperling. "Digital Identification: A Key to Inclusive Growth." McKinsey Global Institute, January 2019. https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

Wiley, Matt. "What Is Header Data?" Equifax, February 22, 2021.

Wilson, Kea. "Zoomers Are Less Likely to Get Drivers Licenses — But They May Not Shift America's Transportation Culture." *Streetsblog USA* (blog), June 3, 2024. https://usa.streetsblog.org/2024/06/03/zoomers-are-less-likely-to-get-drivers-licenses-but-they-may-not-shift-americas-transportation-culture.

Wodecki, Ben. "Visa Uses Generative AI to Catch Suspicious Financial Transactions." AI Business, May 9, 2024. https://aibusiness.com/verticals/visa-uses-generative-ai-to-catch-suspicious-financial-transactions.

Won, Julie, and Jessica Ramos. "Op-Ed: It's Time for New York Banks to Accept IDNYC." *amNY*, April 10, 2024, sec. Op-Ed. https://www.amny.com/opinion/its-time-for-new-york-banks-to-accept-idnyc/.

Worldcoin. "Worldcoin Whitepaper." Accessed September 26, 2024. https://whitepaper.worldcoin.org/.

Yodlee. "Bank Identity Verification | Verify Customer Account Holder Details." Yodlee. Accessed September 18, 2024. https://www.yodlee.com/account-verification/bank-identity-verification.

Additional Acknowledgments

A convening that FinRegLab held jointly with the Aspen Institute's Financial Security Program (FSP) to explore the financial inclusion implications of identity proofing and transaction monitoring was supported by Visa.

Visa (NYSE: V) is a world leader in digital payments, facilitating transactions between consumers, merchants, financial institutions and government entities across more than 200 countries and territories. Our mission is to connect the world through the most innovative, convenient, reliable and secure payments network, enabling individuals, businesses and economies to thrive. We believe that economies that include everyone everywhere, uplift everyone everywhere and see access as foundational to the future of money movement. Learn more at visa.com.

Digital version available at finreglab.org

Published by FinRegLab, Inc.

1701 K Street NW, Suite 1150
Washington, DC 20006
United States