.MAXINE WATERS, CA
CHAIRWOMAN

PATRICK MCHENRY, NC
RANKING MEMBER

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

July 13, 2021

Memorandum

To: Members, Committee on Financial Services
From: FSC Majority Staff
Subject: July 16, 2021, Task Force on Artificial Intelligence Hearing entitled, "I Am Who I Say I Am: Verifying Identity while Preserving Privacy in the Digital Age"

The Task Force on Artificial Intelligence of the House Financial Services Committee will hold a hearing entitled, "I Am Who I Say I Am: Verifying Identity while Preserving Privacy in the Digital Age," on July 16, 2021, at 12:00 p.m. ET, on the virtual meeting platform Cisco Webex. This single-panel hearing will have the following witnesses:

- **Mr. Jeremy Grant**, Coordinator, Better Identity Coalition
- **Mr. David Kelts**, Director of Product Development, GET Group North America
- **Dr. Louise Maynard-Atem**, Research Lead, Women in Identity
- **Professor Elizabeth Renieris**, Founding Director, Notre-Dame-IBM Technology Ethics Lab, University of Notre Dame
- **Mr. Victor Fredung**, Chief Executive Officer, Shufti Pro

Overview

As our society and economy move increasingly online – from banking services to online investing to digital housing products and services – digital verification of an individual's identity is becoming more important to securely facilitate access to essential products and services. Digital payment apps have grown in use domestically and globally, with technological advances allowing smartphone users to make financial transactions that settle faster with just a few steps.[1] The widespread adoption of online banking and other digital products has accelerated due to the COVID-19 pandemic.[2] Simultaneously, the sharp increase in identity theft in the past few years, with the FTC receiving over 1.3 million reports in 2020, up from around 650,000 in 2019, has renewed calls for improvements to digital authentication.[3]

Artificial Intelligence (AI) and other emerging technologies can improve modern smartphones' processing and sensor capabilities and enable the creation of a high quality and privacy-preserving secure digital identity (ID). Smartphone technology companies have begun supporting advanced digital ID products, but with federal and state governments and the private sector each moving at their own pace, interoperability requirements and standards are an issue for hearing review.[4] This hearing will also discuss the future of digital identity frameworks, examining how the emerging technologies (including AI, blockchain, and other distributed ledger technology) could contribute to building digital ID.

---

[1] Yahoo, Digital Payments Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026) (Apr. 19, 2021).
[2] CNBC, Coronavirus crisis mobile banking surge is a shift that's likely to stick (May 27, 2020).
[3] Office of the New York State Comptroller, The Increasing Threat of Identity Theft (May 2021).
[4] *See e.g.*, Vox, Digital driver's licenses are coming: Apple and several states are making digital driver's licenses a reality (Jun. 9, 2021).

Use of Artificial Intelligence in Financial Services

AI can be thought of as computerized systems that work and react in ways commonly thought to require intelligence, while machine learning (ML) algorithms, a type of AI, automatically improve their performance through experience with little or no human input.[5] The financial sector has increased the use of these complex techniques to: (1) facilitate financial crime compliance, including the processes required for customer identification and onboarding, due diligence, transaction monitoring, and investigations into fraud and other financial crime, allowing for rapid identification of patterns and anomalies; (2) personalize consumer services; (3) make credit decisions; (4) inform risk management forecasting and auditing; and (5) identify potential cybersecurity and insider threats.[6]

AI is currently utilized by some financial institutions when collecting, analyzing, and monitoring attributes used to establish and verify digital identities. As a regulated industry, the financial services sector is required to comply with Customer Identification Program and Know Your Customer mandates to verify a customer's true identity.[7] Some financial institutions utilize AI to confirm a customer's identity, by collecting and analyzing traditional, publicly-available data (e.g., a consumer's name or address) together with non-traditional data (e.g., a device's IP address) and biophysical biometric data (e.g., face or fingerprint matching).[8] A newer type of attribute from which AI can infer identity includes behavioral biometrics such as "an individual's email or text message patterns, mobile phone usage, geolocation patterns, and file access log."[9] Both the collection and use of all types of consumer data comes with varying reliability and privacy risks.[10] Collaborative models seek to use AI and ML to enable financial institutions to learn from the data of similar financial institutions and jurisdictions, creating a larger pool of data in which to find patterns and anomalies without moving the data.[11] AI is also used to more accurately evaluate risk related to customers, thereby enabling financial institutions to onboard a broader range of customers, including the unbanked and underbanked.[12]

Identity Proofing

Identity proofing, which is the process of establishing that a subject is who they claim to be, is the first step of establishing a digital identity.[13] The National Institute of Standards and Technology (NIST) has established key outcomes of identity proofing a person: (1) identity *resolution*, where the person is uniquely identified in the context of a population; (2) identity *validation*, where supplied documents are determined to be genuine and accurate; and (3) identity *verification*, where it is confirmed that the person supplying the documents matches the identity claimed on the documents.[14]

---

[5] *See* CRS, Overview of Artificial Intelligence (Oct. 24, 2017); *see also* McKinsey Quarterly, The Economics of Artificial Intelligence (Apr. 24, 2018).
[6] Federal Reserve, FDIC, CFPB, NCUA, OCC, Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning (Mar. 29, 2021); *see also* McKinsey, AI-bank of the future: Can banks meet the AI challenge? (Sep. 2020).
[7] FDIC, Five Things You Should Know About Customer Identification Programs (Feb. 2012). ACAMS, AML Glossary of Terms (last accessed Jul. 6, 2021).
[8] Business Insider, The impact of artificial intelligence in the banking sector & how AI is being used in 2021 (Jan. 13, 2021); *see also* Forbes, PayPal 'Critical' Login Hack: New Report Warns You Are Now At Risk From Thieves (Feb. 22, 2020).
[9] Financial Action Task Force, Digital Identity, (Mar. 2020).
[10] *Id.*
[11] Consilient, Consilient Bank Trials Demonstrate Federated Machine Learning Improves Effectiveness and Efficiency for Financial Crime Detection (Feb. 10, 2021).
[12] The Fintech Times, Driving Financial Inclusion Through Compliance: Helping the Underserved (Nov. 4, 2020)
[13] NIST, Digital Identities Guidelines, Special Publication 800-60-3, (June 2017).
[14] *Id*.

Today, the financial industry often uses "liveness checks" to achieve the third objective (verification) of remote identity proofing in an effort to stop bad actors from opening accounts with stolen but authentic information. These liveness checks involve AI-enabled analysis of a digital self-portrait (or "selfie"), an automated active assessment with a smartphone camera where the user is asked to move their head in a specific direction or blink, or a live video chat with the user.[15]

Synthetic identity fraud, where a bad actor uses a combination of personally identifiable information to fabricate a person or entity, is a driving force behind the money and time that the financial industry spends on identity proofing.[16] It has been estimated that synthetic identity fraud could comprise up at 2.7% of all new accounts and average 4.6 times a typical credit loss.[17] In a typical synthetic identity fraud case, a bad actor might use a nonactive social security number (SSN) in combination with a fake name and addresses in order to apply for financial services.[18]

Even though SSNs were not meant to be a form of national identification, financial service and housing providers often use SSNs for identity proofing purposes.[19] Ever-increasing data breaches of financial institutions and entities that hold SSNs have exemplified the limitations of using SSNs for identification. For example, the Equifax data breach of 2020 comprised the SSNs of nearly 60% of Americans over the age of 18.[20] Today, SSNs can be bought and sold by malicious actors on the dark web for less than $5.00.[21]

Authentication

While identity proofing happens during the initial interaction between a financial institution and a user, authentication occurs each time the user requests a transaction to protect against unauthorized access. The Federal Financial Institutions Examination Council[22] (FFIEC) has recommended regulated financial institutions utilize two or more types of authentication (also known as multi-factor) to validate users.[23] Three common factors used for authentication include: (1) something you know, (2) something you have, or (3) something you are.[24] The first type, something you know, are the most commonplace—passwords and passcodes (e.g., PIN numbers) are used for many user accounts. Other financial institutions may utilize something you have, like a one-time code generated from authenticator mobile applications or hardware tokens. Financial institutions may also use biometric authenticators, or something you are, for account access, particularly via a bank provided mobile application.

Issues of Privacy and AI Bias

Methods used by entities to verify an individual's digital ID in order to provide access to housing or financial services raise various concerns regarding an individual's privacy, algorithmic bias, and

[15] ACAMS, E-KYC in the Digital Era (Sep. 30, 2020).
[16] The Federal Reserve – FedPayments Improvement, Synthetic Identity Fraud Defined (accessed Jul. 12, 2021).
[17] The Federal Reserve – FedPayments Improvement, Mitigating Synthetic Identity Fraud in the U.S. Payment System (Jul. 2020).
[18] Experian, Synthetic identity fraud update: Effects of COVID-19 and a potential cure from Experian (Sep. 15, 2020).
[19] The Verge, Identity crisis: how Social Security numbers became our insecure national ID (Sep. 26, 2012).
[20] *Id.*
[21] *Id*. The July 2017 breach at Equifax, which resulted in the loss of personal information of an estimated 148 million U.S. consumers and most recently, the Capitol One Security Incident that affected 100 million individuals in the US than accounts being compromised. *See* FTC, Equifax Data Breach Settlement (Jan. 2020); *see also* Capital One, Information on the Capital One Cyber Incident (Aug. 4, 2019).
[22] FFIEC is comprised of the Federal Reserve, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Consumer Financial Protection Bureau.
[23] Bank Info Security, FFIEC Guidance: Multifactor Authentication and Layered Security (Jun. 6, 2011).
[24] Pearson, Understanding the Three Factors of Authentication (Jun. 6, 2011).

inclusion. For example, with many housing and financial services providers collecting sensitive personal information from consumers electronically, cybersecurity hacks have already put millions of consumers at risk of identity fraud. The use of AI and big data analytics for individual identification and subsequent decision-making has also raised concerns about algorithmic bias.[25] For example, smartphone authentication often uses voice and facial recognition technologies that have historically exhibited bias against women and minorities.[26] Further, if data used to train AI systems contain biases and inaccuracies, individuals are at risk of being improperly denied access to benefits such as credit, housing, or social services.[27] Obtaining recourse in such instances, or preventing them in the first place, can be challenging because complex AI systems have been criticized for being opaque, non-intuitive, and difficult for people to understand.[28] Additionally, stakeholders such as the American Civil Liberties Union have raised privacy concerns about how a digital ID could enable centralized tracking, or allow sensitive consumer data to be shared with third-parties.[29]

The Potential For Inclusion

One study found that roughly 11% of U.S. citizens, comprising 21 million people, did not have government-issued identification, and pointed to the cost of document fees, travel expenses, and waiting times, acted as a deterrent to receiving identification.[30] Currently, obtaining a government-issued ID requires on complex, time-consuming, and often costly processes of collecting official copies of various documents (e.g., SSN card, birth certificate, marriage licenses) through numerous postal mail and in-person visits.[31] Some stakeholders have suggested that a digital ID system could help ensure that everyone can have a valid form of identification that is widely accepted by simplifying processes for application and replacement.[32] Additionally, a secure digital identity system could help facilitate better consumer data sharing between financial institutions and foster more open banking, thereby possibly increasing financial inclusion.[33]

Mobile Driver's Licenses

The International Organization for Standardization has convened a diverse group of stakeholders, including representatives from government, academia, industry, and law enforcement, to draft the ISO 18013-5 mobile driving license (mDL) standard.[34] Several states have implemented mobile driver's license pilot programs, including Utah, Iowa, and Florida, with some advocates arguing that the unprecedented coronavirus pandemic necessitated the adoption of contactless identification methods due to public health concerns. [35] Some pilots came out of a partnership between NIST and the private sector to create a digital driver's license while others are implementing the ISO 18013-5 standard.[36] While these pilot projects vary, users generally are able to access their mobile identity with a passcode, or by using their smartphone's

[25] For discussions of biases in AI algorithms and data sets, *see e.g.*, Rachel Courtland, Bias detectives: the researchers striving to make algorithms fair, Nature (Jun. 20, 2018).
[26] *See e.g.*, Harvard Business Review, Voice Recognition Still Has Significant Race and Gender Biases (May 10, 2019).
[27] *See e.g.*, FTC, Big Data: A Tool for Inclusion or Exclusion? (Jan. 2016).
[28] Matt Turek, Explainable Artificial Intelligence (XAI), Defense Advanced Research Projects Agency (accessed Jul. 2, 2021).
[29] ACLU, Identity Crisis: What Digital Driver's Licenses Could Mean For Privacy, Equity, And Freedom (accessed Jul. 12, 2021).
[30] Brennan Center for Justice, Citizens Without Proof: A Survey Of Americans' Possession Of Documentary Proof Of Citizenship And Photo Identification (Nov. 2006).
[31] *See* Star Tribune, Real frustrations pile up over obtaining a Real ID (Jan. 29, 2020); *see also* Newsday, Some citizens are facing hurdles to get REAL ID (Mar. 9, 2020).
[32] *See e.g.*, World Bank, Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable (Aug. 14, 2019); *see also* McKinsey, Digital identification: A key to inclusive growth (Apr. 17, 2019).
[33] Accenture, Digital identity in the post-COVID era – how Open Banking can help (Dec. 16, 2020).
[34] Google, Privacy-preserving features in the Mobile Driving License (Oct. 28, 2020).
[35] AP, Pandemic gives boost as more states move to digital IDs (May 8, 2021).
[36] NIST, Pilots (accessed Jun. 29, 2021); *see also* GET Group, Utah Launches Pioneering Pilot on Mobile Driver's License (Mar. 30, 2021).

facial or fingerprint recognition; but, some privacy-preserving versions allow users to share only select elements of their identity. For example, if a user needed to prove they were over the age of 18 to a merchant, a privacy-preserving digital ID could cryptographically confirm they were over 18 without sharing an exact month and day of birth.

In 2019, Google announced it was working on the ability to securely add compatible digital versions of real-world identifications in their mobile smartphone wallet on Android phones.[37] In October 2020, Google provided an update that Android 11 operating systems can support the international mDL standard.[38] In June 2021, Apple announced a similar feature—iPhones would also soon have the capacity to hold a digital version of compatible government-issued forms of identification.[39] Any compatible digital ID would be encrypted and integrated within the same hardware technology as Apple Pay, which provides mobile payment options.[40]

Use of Blockchain Technology

Other technology companies such as IBM[41] and Microsoft[42] have conducted research on using a public permissioned blockchain ledger for identity verification. Some nations such as Estonia[43] and Singapore[44] have unveiled decentralized identity pilot projects that utilize blockchain technology. If these pilots use decentralized data systems (such as self-sovereign identity proposals or blockchain identity systems) where the information is securely stored on an individual's device in a digital wallet, this would still require strong passwords for user log-in, but could be susceptible to hacks.[45]

Recent Proposals and Regulatory Activity on Digital Identity Verification

In February 2021, the Treasury Department held a financial sector innovation policy roundtable, which brought together experts to discuss "how innovations like interoperable, privacy-preserving digital identity solutions, and more effective anti-money laundering and anti-fraud mechanisms."[46] Regarding the use of AI in the financial services industry, in December 2018, the Federal Reserve, FDIC, FinCEN, NCUA, and OCC released a joint statement that noted, "[s]ome banks are also experimenting with artificial intelligence and digital identity technologies applicable to their BSA/AML compliance programs. These innovations and technologies can strengthen BSA/AML compliance approaches, as well as enhance transaction monitoring systems."[47] In October 2020, the Consumer Financial Protection Bureau (CFPB) released an Advance Notice of Proposed Rulemaking, asking the public how it might most efficiently and effectively develop regulations to implement Section 1033 of the Dodd-Frank Act, which provides for consumer rights to access financial records. The CFPB stated that, "growth in authorized data access has been accompanied by expansion in the number of distinct applications or 'use cases' for authorized data, including, but not limited to, … identity verification and account ownership validation."[48]

---

[37] Venture Beat, Google is bringing Electronic IDs to Android (May 9, 2019).
[38] Google, Privacy-preserving features in the Mobile Driving License (Oct. 28, 2020).
[39] Apple, iOS 15 brings new ways to stay connected and powerful features that help users focus, explore, and do more with on-device intelligence (Jun. 7, 2021).
[40] *Id.*
[41] IBM, IBM Verify Credentials: transforming digital identity into decentralized identity (accessed Jun. 29, 2019).
[42] Microsoft, Partnering for a path to digital identity (Jan 22, 2018).
[43] PWC, Estonia – the Digital Republic Secured by Blockchain (2019).
[44] GovInsider, Exclusive: How Singapore is building a privacy-based digital ID (Sep 28, 2020).
[45] *See* World Economic Forum, A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity (Aug. 2016).
[46] Treasury, U.S. Treasury Department Holds Financial Sector Innovation Policy Roundtable (Feb 10., 2021).
[47] Federal Reserve, FDIC, FinCEN, NCUA, and OCC, Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (Dec. 3, 2018).
[48] CFPB, A Proposed Rule on Consumer Access to Financial Records (Nov. 6, 2020).