MAXINE WATERS, CA
CHAIRWOMAN

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

PATRICK MCHENRY, NC
RANKING MEMBER

September 9, 2019

Memorandum

To: Members, Committee on Financial Services

From: FSC Majority Staff

Subject: Thursday, September 12 at 9:30 AM, "The Future of Identity in Financial Services: Threats, Challenges, and Opportunities."

The Task Force on Artificial Intelligence of the House Financial Services Committee will hold a hearing entitled, "The Future of Identity in Financial Services: Threats, Challenges, and Opportunities," on September 12 at 9:30 AM a.m. in Room 2128 of the Rayburn House Office Building. This single-panel hearing will have the following witnesses:

- **Anne Washington,** Assistant Professor of Data Policy, NYU Steinhardt School
- **Valerie Abend,** Managing Director, Accenture Security
- **Jeremy Grant,** Coordinator, Better Identity Coalition
- **Amy Walraven,** President and Founder, Turnkey Risk Solutions
- **Andre Boysen**, Chief Identity Officer, SecureKey Technologies

Overview
The way that consumers identify themselves and have their identities verified in the financial marketplace, particularly online, has evolved in recent years. The "digital identity," which is typically a combination of a username and password, allows a user to access an IT system connected to the internet. IT systems connected to the internet within the financial services industry, where laws and regulations require entities to know who their customers are, typically must also authenticate individuals. Authentication generally involves (1) something you know, (2) something you have, (3) something you are. Some authentication procedures may require, two-steps to authenticate an individual, commonly referred to as multifactor authentication. At the authentication stage, artificial intelligence (AI) plays a critical role in utilizing algorithms and other technologies to analyze databases to ensure the user creating or using the account is the actual user.[1]

At the same time, the convenience brought by digital identities to financial services is not without risk. Individual customers can fall victim to bad actors using illicitly obtained and publicly available information to trick AI systems (voice authentication, customer service chat bots, etc.) into validating them instead of the actual customers. Similarly, companies are also subject to bad actors attempting to gain authorized access to their systems by creating wholly false ("synthetic") identities, misusing employee log-in credentials, or compromising digital infrastructures. Moreover, the digital identity

[1] This memo was prepared with the assistance of Chris Jaikaran and Laurie A. Harris from the Congressional Research Service (CRS).

landscape in financial services has varied layers that require different goals for confirming identity and along the way, each layer has a distinctive problem associated with achieving that goal.[2]

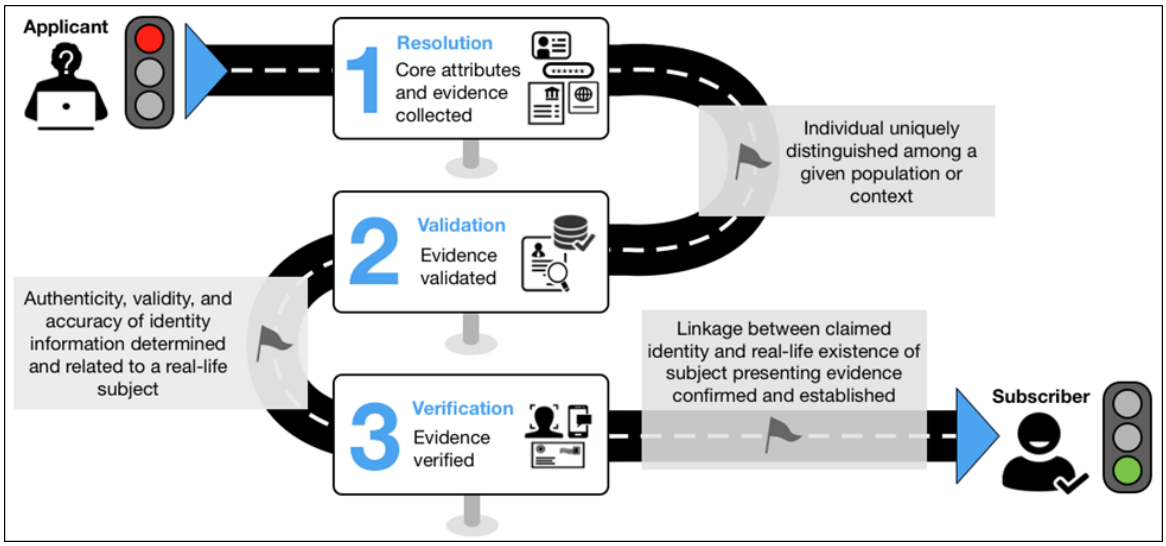
Terminology in Digital Identification

There are basic entities and concepts that make up the digital-identity ecosystem. For the financial services industry, the following terms and concepts are frequently used:

1. *Credentialing Service Provider* ("CSP") is a trusted entity that issues or registers applicants' authenticators and issues credentials after completing Customer Identification Program ("CIP") and/or know-your-customer ("KYC") requirements.[3] A CSP may be an independent third party or issue credentials for its own use.[4]
2. *Identity Proofing* is a process that, at a minimum, requires an applicant to provide a form of identification, a CSP to validate the information provided (check it against databases, etc.), and some form of verification (visiting a bank or sending a picture of a driver's license passport).[5]
3. *Access control* is the process for using a digital identity after it has been proofed and authenticated by the CSP. Cryptographic and integrity-checking mechanisms are used to determine whether a digital identity: (1) is valid; (2) should be allowed access; and (3) has restrictions on which parts of a system the identity may or may not access.[6]

Further, the National Institute of Standards and Technology (NIST) outlined the basic flow for identify proofing and enrollment, as shown in the graphic below.

Figure 1. NIST Process flow for identity proofing[7]



[2] For example, the World Economic Forum posits six different layers within financial services: (1) standards, (2) attribute collection, (3) authentication, (4) attribute exchange, (5) authorization, and (6) service delivery. Each layer has the respective problem: (1) lack of consistency (2) inaccurate collection, (3) weak authentication, (4) insecure exchanges, (5) complex rules, and (6) inefficient service. *See*, R. Jesse McWaters, "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity", at http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[3] FinCEN, "USA Patriot Act, Section 326: Verification of Identification" https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.

[4] NIST, "Appendix A—Definitions and Abbreviations", https://pages.nist.gov/800-63-3/sp800-63-3/definitions.html

[5] NIST, "Digital Identity Guidelines: Enrollment and Identity Proofing," SP 800-63A, June 2017, at https://doi.org/10.6028/NIST.SP.800-63a.

[6] CRS Report R44642, "Encryption: Frequently Asked Questions" at https://fas.org/sgp/crs/misc/R44642.pdf

[7] *Id*.

Authentication. Broadly, authentication is often conflated with identity proofing; however, within financial services, authentication refers to the process of a CSP validating a digital identity presented to it and granting access to the parts of the system for which that identity is authorized.[8] This translates into financial institutions granting access after users enter (1) passwords, (2) credentials to validate an owned item (smartphone or debit card) and the user identity, or (3) biometric identifiers; respectively.[9] To provide more robust protection for customers, the financial service industry has long combined the single-factor authenticators mentioned above to create multi-factor authentication. For example, when a customer uses an ATM, they are required to present something they know (typically a 4-digit pin) and something they have (debit card or smartphone) to complete the transaction. Despite the strength of multi-factor authenticators, the process still depends on users not becoming "password fatigued" and users creating complex passwords.[10]

One popular method for authentication is the Social Security Number ("SSN"). However, since its creation, the SSN has also expanded to serve as an identifier rather than exclusively as an authenticator because it is not so much of a secret as it originally functioned. Today, consumers frequently share their SSNs with many financial institutions and other businesses.[11] As an authenticator, SSN's are used to determine whether a certain person claiming to be a certain person is in fact that certain person. Comparatively, identifiers within a digital infrastructure are used to determine what account belongs to which person. Yet, as data breaches of financial institutions and entities that hold SSNs become more common, the clandestine nature of SSNs is lost. For example, the Equifax data breach comprised the SSNs of nearly 60% of Americans over the age of 18.[12] SSNs are also bought and sold by malicious actors on the dark web for less than $5.00.[13]

Proposals to solve this problem include removing SSN's from documents and materials when they are not necessary, replacing SSNs with other authenticators or identifiers, or creating a nationwide or centralized database. There are inherent risks and positives with each policy solution; moreover, in one case study from the healthcare industry, a company used a combination of all three to implement a better SSN policy.[14] Additionally, one popular solution among the industry is decentralized data systems (also known as "self-sovereign identity proposals" or "blockchain identity systems") where broadly, the information is securely stored on an individual's device in a digital wallet,[15] but would still require strong passwords for user log-in and can be susceptible to hacks.

Artificial Intelligence ("AI") and Data Security. In financial services, AI is utilized in collecting, analyzing, and monitoring the attributes used to establish and verify digital identities and subsequently

---

[8] *See generally*, BRT, "BRT Releases Recommendations for Strengthening Digital Identity, Reducing Identity Theft and Fraud", at https://s3.amazonaws.com/brt.org/BRT-DigitalIDReportJuly2019.pdf.
[9] *See generally*, id.
[10] Brian Krebs, "The Risk of Weak Online Banking Passwords," Krebs on Security, Aug. 19, 2019 at https://krebsonsecurity.com/2019/08/the-risk-of-weak-online-banking-passwords/.
[11] *See*, The Better Identity Coalition, "Better Identity in America: A Blueprint for Policymakers," July 2018, at https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5d419caa5001d70001614b8f/1564581036670/Better_Identity_Coalition%2BBlueprint%2B-%2BJuly%2B2018.pdf
[12] *See* Better Identity Coalition, *infra* 11.
[13] *See* generally, Better Identity Coalition, *infra* 11. 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" at https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement and Capital One, "Information on the Capital One Cyber Incident," Aug. 4, 2019, at https://www.capitalone.com/facts2019/.
[14] In 2014, Aetna launched the SSN Protection, Elimination, and Remediation (SPEAR) initiative which is claims has reduced the use of SSN. Aetna, "Our Effort to Reduce the Use of SSNs," at https://www.aetna.com/legal-notices/privacy/effort-to-reduce-use-social-security-numbers.html.
[15] *See* R Jesse McWaters, *infra* 2 and Business Roundtable, *infra* 8.

detect and address fraudulent activities. Additionally, AI systems may also be used to rapidly analyze large, ever-growing data sets and points. For example, a bank could use AI to confirm a customer's identity, after suspicious activity occurs in their account, by collecting and analyzing traditional data (e.g., Social Security number, name, address) together with non-traditional data (e.g., social media posts and location information) and biometric data (e.g., from face and voice recognition technologies); this could provide identity validation efficiently with increased confidence. More specifically, utilizing these data points, the bank could know that Person A living in Los Angeles, CA, is not in Las Vegas trying to withdraw $2000 from a casino.[16]

At the same time, the same databases that banks (some are public) use to confirm a customer's identity are susceptible to malicious actors. Data breaches, particularly ones where large amounts of personally identifiable information (PII) are exposed, provide much of the information that a bad actor may need to open an account with a company, especially if that company uses credit reporting agency information in their data-verification process.[17] This is concerning because about 40% of adults say they use the same passwords on accounts and share that same password with friends and family on accounts.[18] The criminal actions after a data breach often work as follows: after a bad actor creates one account with information stolen from a data breach, other accounts are created (with fake documents, likely sourced from public databases) from which the criminal can steal the assets from the legitimate account and send them to additional, falsely obtained accounts before using or withdrawing the assets.[19]

Companies are also susceptible to data breaches. A criminal may compromise an employee's digital identity using the tactics discussed above. Then, the criminal may use the employee's credentials to further infiltrate internal operating systems, like human resource records. In addition to protecting employee credentials, companies must also ensure that the credentialing processes of their third-party providers are robust. Third-party providers in the financial services sector work for many institutions simultaneously and present a unique risk to the sector.[20] This is concerning because over the past few years, there is a growing reliance on third-parties by financial institutions to complete integral operational services.[21] As stated in the Financial Stability Oversight Council's 2018 Annual Report, "These services have information and cost benefits, but relying on outside firms for critical data and services also creates risks."

Synthetic fraud (or wholly false identities) which involves bad actors using a combination of fake information, such as a fictitious name, and real data like a child's social security number to create a synthetic ID, plays an increasing role in permitting bad actors to steal and launder money faster and without detection.[22] Synthetic fraud is difficult to track once the synthetic ID is created, fraudsters can obtain loans and other credit products, create fictious companies, and move illicitly obtained funds to accounts under the bad actors' control.[23]

---

[16] Tim Sloane, "!8 Top Use cases of AI in Banks", Nov. 6, 2018, at https://www.paymentsjournal.com/the-18-top-use-cases-of-artificial-intelligence-in-banks/.
[17] *See* FTC and Capital One, *infra* 12.
[18] See Aaron Smith, "AMERICANS AND CYBERSECURITY: Password management and mobile security", Jan. 26, 2017, at https://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/.
[19] See generally, Lily Hay Newman, "The WIRED Guide to Data Breaches", Dec. 7, 2018, at https://www.wired.com/story/wired-guide-to-data-breaches/.
[20] Financial Stability Oversight Council, "2018 Annual Report" annual report, June 20, 2019, at https://home.treasury.gov/system/files/261/FSOC2018AnnualReport.pdf.
[21] *Id.*
[22] Bev O'Shea, "What is Synthetic Identity Theft?", Nerd Wallet, Apr. 27, 2019, at https://www.nerdwallet.com/blog/finance/synthetic-identity-theft/
[23] See generally, Federal Reserve, "Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors" Jul. 11, 2019, at https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

Regulatory Challenges. There are a variety of federal and state laws pertaining to data protection and privacy,[24] however there is no federal law that mandates financial institutions to implement multi-factor authentication or diversify their technology providers. Most notably for the financial marketplace, the Gramm-Leach-Bliley Act ("GLBA") requires financial institutions to safeguard nonpublic personal information, though the law does not provide a private right of action.[25] The principle of market discipline would suggest that institutions with poor security practices will be unsuccessful because consumers would not trust them and take their business elsewhere. However, in some circumstances, a consumer may not necessarily choose to use a company that has their data, such as a credit reporting agency.[26] Moreover, as new and non-traditional companies enter the financial sector and privacy policies become longer and more complicated, it may become difficult for consumers to differentiate between companies.

Further, financial institutions face a range of regulations affecting the operations of those institutions.[27] The Federal Financial Institutions Examination Council ("FFIEC") provides guidance to financial institutions on the security of accessing accounts on IT systems.[28] However, FFIEC states that it is up to institutions to assess risk and determine the appropriate actions for their systems. This means that each bank can run an entirely separate privacy program for review by each federal agency.

[24] CRS, *Data Protection Law: An Overview*, March 25, 2019
[25] FTC. "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act," at https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.
[26] See FSC Full Committee Hearing, *Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System*, Feb. 26, 2019.
[27] For an example, see the Office of the Comptroller for the Currency "Comptroller's Handbook" at https://www.occ.treas.gov/publications/publications-by-type/comptrollers-handbook/index-comptrollers-handbook.html.
[28] FFIEC, "II.C.16 Customer Remote Access to Financial Services," *FFIEC IT Examination Handbook InfoBase*, at https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic16-customer-remote-access-to-financial-services.aspx. FFIEC, "II.C.7(b) User Access Programs," *FFIEC IT Examination Handbook InfoBase*, at https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(b)-user-access-program.aspx.