PATRICK MCHENRY, NC
CHAIR

MAXINE WATERS, CA
RANKING MEMBER

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

September 6, 2023

The Honorable Janet Yellen
Secretary
U.S. Department of the Treasury
1500 Pennsylvania Ave. NW
Washington, DC 20220

The Honorable Todd Harper
Chairman
National Credit Union Association
1775 Duke Street
Alexandria, VA 22314

The Honorable Martin Gruenberg
Chairman
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Ms. Andrea Gacki
Director
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Mr. Michael Hsu
Acting Comptroller
Office of the Comptroller of the Currency
400 7th Street, SW, Suite 3E-218
Washington, DC 20219

The Honorable Jerome Powell
Chairman
Board of Governors of the Federal Reserve System
20th Street & Constitution Ave, NW
Washington, DC 20551

Dear Secretary Yellen, Director Gacki, Chairman Gruenberg, Chairman Harper, Acting Comptroller Hsu, and Chairman Powell:

I write today to request that the Financial Crimes Enforcement Network, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the United States Department of the Treasury ("Agencies") examine the Customer Identification Program ("CIP") mandates for opportunities to modernize the related rule's requirements for complying financial institutions ("banks"). This is in light of changes to both the business of banking and the technologies and analytic capabilities available to banks that have been developed since the 2003 issuance of 31 CFR 1020.220 ("CIP Rule").[1] This request is also inspired by concern about the security of consumers' personal data, given the frequent targeting of banks by malicious cyber actors.[2]

As you know, per statute and designed to protect our nation's security,[3] under the CIP Rule, banks are required to implement a CIP that includes risk-based verification procedures that enable the bank to form a reasonable belief that it knows the true identity of its customers. These procedures must specify what identifying information the bank will collect from each customer, prior to establishing an account. The minimum information under CIP includes a customer's name, date of birth, address, and identification number (for U.S. persons, typically, a social security number ["SSN"]). The CIP procedures must also contain risk-based procedures for verifying the identity of the customer through documentary or non-documentary methods.

In order to accomplish this, the rule currently requires that:

> [t]he bank must obtain, at a minimum, the following information *from the customer* prior to opening an account:
>
> (1) Name;
> (2) Date of birth, for an individual;
> (3) Address, which shall be:
>
> (i) For an individual, a residential or business street address;

[1] FinCEN, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, "Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks," 68 FR 25090 (Final Rule, May 9, 2003).
[2] Carnegie Endowment for International Peace, Timeline of Cyber Incidents Involving Financial Institutions. (Accessed August 27, 2023)
[3] The CIP Rule implements Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.

(ii) For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual; or

(iii) For a person other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location; and

(4) Identification number, which shall be:

(i) For a U.S. person, a taxpayer identification number; or

(ii) For a non-U.S. person, one or more of the following: A taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.[4]

I understand that the CIP rule's requirement to collect a taxpayer identification number is being interpreted by some regulators to mean that when collecting the SSN, they must collect from customers the *full* nine-digit number. This made sense when the CIP rule was issued 20 years ago, but today, using advanced identification tools, banks have other means of leveraging minimally collected information to enhance their reasonable belief of the customer's true identity. For example, a bank might collect only the last four digits of a customer's SSN as part of an online application, and using address, date of birth, and other publicly available information, it can obtain the first five digits through third-party identification tools. Such tools can also allow for cross-referencing of customer information to analyze email addresses, phone numbers, and internet protocol ("IP") address location to discern a customer's identity. Banks may use multifactor authentication (e.g., emailing a code to a provided email address), as well. With the advent of online banking and online applications for credit and accounts, these tools may be an important and useful part of a bank's CIP.

Further, while new technology is available to help banks, it is also available to help those who would target institutions to steal customers' personally identifiable information. This includes the SSNs of customers, collected to fulfill the CIP rule requirements. Banks report a growing reluctance of consumers to offer their full nine-digit SSN due to the risks associated with identity theft and data breaches in order to obtain credit and other banking services.[5] For example, in 2017, Equifax experienced one of the largest data breaches, exposing SSN and other sensitive personal data of 147 million individuals.[6] In 2021, more than 100 companies, including Morgan Stanley and Flagstar Bank, were hacked and had customer SSN and other sensitive data stolen.[7] In 2022, Flagstar Bank was hacked again and had 1.5 million customer SSN data stolen.[8]

In light of these data breaches, cybersecurity and data privacy experts have urged companies and policymakers to prioritize data minimization to ensure businesses are only collecting the data they need to provide a product or service.[9] Moreover, the current CIP rules already allow flexibility for credit card companies to collect only 4 digits of a customer's SSN when the company uses third-party identification tools, and it seems prudent to consider formally expanding that flexibility to applications for other financial services and products.

Accordingly, I ask that your Agencies consider issuing new Frequently Asked Questions ("FAQs"), a change to the Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering Manual, and/or other administrative improvements to reflect these modern technologies and concerns. Specifically, I request that your Agencies consider whether it is appropriate to allow for the collection of only four digits of the customer's SSN directly from the applicant when they use other appropriate tools to ensure proper identification. Banks choosing to collect four

---

[4] 31 CFR 1020.220(a)(2)(i)(A) (emphasis added).

[5] Customers are aware of data losses from high-profile breaches across industry. In general, headlines remind all of us that "Following breaches at Capital One, Equifax and a slew of other financial and healthcare organizations, there's little doubt that your social security number has been compromised. . ." (https://www.forbes.com/sites/suzannerowankelleher/2019/08/01/everyones-social-security-number-has-been-compromised-heres-how-to-protect-yourself/?sh=f77a7c29ac7e

[6] FTC, *Equifax Data Breach Settlement* (Dec. 2022).

[7] See SC Magazine, *Accellion claims no 'guarantee' of security in $8.1M breach settlement* (Jan. 14, 2022); TechCrunch, *The Accellion data breach continues to get messier* (Jul. 8, 2021); and TechCrunch, *Hackers stole Social Security numbers in Flagstar data breach affecting 1.5 million customers* (Jun. 21, 2022).

[8] TechCrunch, *Hackers stole Social Security numbers in Flagstar data breach affecting 1.5 million customers* (Jun. 21, 2022).

[9] For example, see Testimony of Samir Jain, Director of Policy, Center for Democracy and Technology

numbers of the SSN would still have to maintain robust and risk-based CIPs and would still have to demonstrate to regulators that the collected information is sufficient to allow the banks to form a reasonable belief that they know the true identity of the customer.

Sincerely,

Maxine Waters
Ranking Member
Committee on Financial Services