DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network

Request for Information and Comment on Customer Identification Program Rule Taxpayer Identification Number Collection Requirement

AGENCY: Financial Crimes Enforcement Network (FinCEN), Treasury.

ACTION: Notice and request for information and comment.

SUMMARY: FinCEN, in consultation with staff at the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Board of Governors of the Federal Reserve System (Board) (collectively, the ''Agencies''), seeks information and comment from interested parties regarding the Customer Identification Program (CIP) Rule requirement for banks to collect a taxpayer identification number (TIN), among other information, from a customer who is a U.S. person, prior to opening an account (the ''TIN collection requirement''). Generally, for a customer who is an individual and a U.S. person (''U.S. individual''), the TIN is a Social Security number (SSN). In this request for information (RFI), FinCEN specifically seeks information to understand the potential risks and benefits, as well as safeguards that could be established, if banks were permitted to collect partial SSN information directly from the customer for U.S. individuals and subsequently use reputable third-party sources to obtain the full SSN prior to account opening. FinCEN seeks this information to evaluate and enhance its understanding of current industry practices and perspectives related to the CIP Rule's TIN collection requirement, and to assess the potential risks and benefits associated with a change to that requirement. This notice also serves as a reminder from FinCEN, and staff at the Agencies, that banks must continue to comply with the current CIP Rule requirement to collect a full SSN for U.S. individuals from the customer prior to opening an account (''SSN collection requirement''). This RFI also supports FinCEN's ongoing efforts to implement section 6216 of the Anti-Money Laundering Act of 2020, which requires FinCEN to, among other things, identify regulations and guidance that may be outdated, redundant, or otherwise do not promote a risk-based anti-money laundering/countering the financing of terrorism (AML/CFT) regime.

DATES: Written comments on this RFI are welcome and must be received on or before May 28, 2024.

ADDRESSES: Comments may be submitted by any of the following methods:

- *Federal eRulemaking Portal: https://www.regulations.gov.* Follow the instructions for submitting comments. Refer to Docket Number FINCEN–2024–0009.
- *Mail:* Policy Division, Financial Crimes Enforcement Network, P.O. Box 39, Vienna, VA 22183. Refer to Docket Number FINCEN–2024–0009.

Please submit comments by one method only.

FOR FURTHER INFORMATION CONTACT: FinCEN's Regulatory Support Section at 1–800–767–2825 or electronically at *frc@fincen.gov.*

SUPPLEMENTARY INFORMATION:

I. Background

A. Bank Secrecy Act

The legislative framework generally referred to as the Bank Secrecy Act (BSA),[1] which consists of the Currency and Financial Transactions Reporting Act of 1970 and other legislation, is designed to combat money laundering, the financing of terrorism, and other illicit finance activity. To fulfill the purposes of the BSA, Congress authorized the Secretary of the Treasury (Secretary) to administer the BSA and require financial institutions to keep records and file reports that, among other purposes, ''are highly useful in criminal, tax, or regulatory investigations, risk assessments, or proceedings,'' or in the conduct of ''intelligence or counterintelligence activities, including analysis, to protect against terrorism.'' [2] The Secretary has delegated the authority to implement, administer, and enforce compliance with the BSA and its implementing regulations to the Director of FinCEN.[3]

Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) [4] amended the BSA to require, among other things, the Secretary to prescribe regulations ''setting forth the minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution.'' [5] These minimum standards include, among other things, reasonable procedures for: (1) ''verifying the identity of any person seeking to open an account to the extent reasonable and practicable''; and (2) ''maintaining records of the information used to verify a person's identity, including name, address, and other identifying information.'' [6]

B. The CIP Rule: Certain Minimum Information Collection Requirements and Risk-Based Identity Verification Procedures

In 2003, FinCEN and the Agencies issued regulations implementing section 326 of the USA PATRIOT Act for banks.[7] Among other requirements, the CIP Rule requires a bank to, as part of its AML program, implement a written CIP that contains identity verification procedures that enable the bank to form a reasonable belief that it knows the true identity of its customers, including by verifying the identity of its customers to the extent reasonable and practicable. These procedures must specify the customer identifying information that a bank is to collect from each customer, including, at a minimum, the customer's name, date of birth (for an individual), address, and identification number. For U.S. persons, the identification number is a TIN.[8] Generally, to fulfill the CIP

[1] Certain parts of the Currency and Foreign Transactions Reporting Act of 1970, its amendments, and the other statutes relating to the subject matter of that Act, have come to be referred to as the Bank Secrecy Act (BSA). These statutes are codified at 12 U.S.C. 1829b, 1951–1960, and 31 U.S.C. 5311–5314, 5316–5336 and includes other authorities in notes thereto. Regulations implementing the BSA appear at 31 CFR chapter X.

[2] 31 U.S.C. 5311(1).

[3] Treasury Order 180–01 (Jan. 14, 2020), Paragraph 3(a), *available at https://home.treasury.gov/about/general-information/orders-and-directives/treasury-order-180-01.*

[4] USA PATRIOT Act, Public Law 107–56.

[5] 31 U.S.C. 5318(*l*).

[6] *Id.,* at 5318(*l*)(2)(A)–(B).

[7] *See, e.g.,* Board, FDIC, OCC, FinCEN, Office of Thrift Supervision, and NCUA, *Joint Final Rule—Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks,* 68 FR 25103 (May 9, 2003) (codified at 31 CFR 1020.220(a)(4)), *available at https://www.federalregister.gov/citation/68-FR-25103.* These regulations are codified under 12 CFR 208.63(b)(2), 12 CFR 211.5(m)(2), and 12 CFR 326.8(b)(2) (FDIC); 12 CFR 211.24(j)(2) (Board); 31 CFR 1020.220 (FinCEN); 12 CFR 748.2(b)(2) (NCUA); and 12 CFR 21.21(c)(2) (OCC) (collectively, the ''CIP Rule''). Additionally, in 2020, FinCEN issued a final rule implementing the CIP Rule for banks that lack a Federal functional regulator. *See* FinCEN, *Customer Identification Programs, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator,* 85 FR 57129 (Nov. 16, 2020) (codified at 31 CFR 1010 and 31 CFR 1020).

[8] *See* 31 CFR 1020.220(a)(2)(i)(A)(*4*); *see also* 31 CFR 1010.100(yy). A TIN is defined by section 6109 of the Internal Revenue Code of 1986 (26 U.S.C. 6109) and the Internal Revenue Service regulations implementing that section (*e.g.,* SSN or employer identification number). In instances in which a U.S. person has not yet received a TIN, the CIP Rule provide an exception for persons applying for a

Continued

Rule's TIN collection requirement for a U.S. individual, a bank must collect from the customer prior to opening an account the full SSN. While a bank's procedures for verifying a customer's identity may be risk-based and may vary from bank to bank, the CIP Rule makes clear that the collection of certain identifying information is a minimum requirement and such information must be collected directly from the customer prior to opening an account, except with respect to credit card accounts. The CIP Rule generally does not provide for a bank collecting an individual's SSN from a person other than the customer (*e.g.,* from a third-party service provider).

When the CIP Rule was adopted, banks were exempted from the requirement with respect to credit card accounts to collect identifying information, including an identification number, directly from the customer. Instead, for credit card accounts, a bank may obtain the customer's identifying information, such as the SSN, from a third-party source prior to extending credit to the customer. FinCEN recognized at that time that without this exception, the CIP Rule would alter a bank's business practices by requiring additional information beyond what was already obtained directly from a customer who opened a credit card account at the point of sale or by telephone.[9] Concerns were raised during the proposed CIP Rule's comment period that an individual applying for a credit card account would be reluctant to give out their SSN, especially through non-face-to-face means, due to consumer privacy and security concerns.[10] FinCEN observed that requiring a bank to collect a customer's identifying information from the customer in every case, including over the phone, would likely alter the manner in which they do business.[11] FinCEN was also mindful of the legislative history of section 326, which indicated that Congress expected implementing regulations be appropriately tailored for accounts opened in situations where the account holder was not physically present at the financial institution and would not impose requirements that were burdensome, prohibitively expensive, or impractical.[12] Therefore, credit card accounts were exempted from the CIP Rule's information collection requirements, allowing banks to obtain a customer's identifying information from a third-party source, such as a credit bureau, prior to an extension of credit. FinCEN considered this practice to be an efficient and effective means of extending credit with little risk that the lender did not know the identity of the borrower.[13]

Since the CIP Rule was adopted in 2003, FinCEN is cognizant that there has been significant innovation in the way that customers interact with financial institutions and receive financial services, as well as significant innovation in the customer identifying information collection and verification tools available to financial institutions.[14] Many banks now partner with non-bank financial institutions (*e.g.,* third-party service providers) to facilitate new financial products and services, such as buy-now-pay-later (BNPL) loans that extend credit at point of sale to customers. These products and services operate in a similar manner to credit cards but may be offered by non-bank financial institutions that may or may not be subject to the BSA and its implementing regulations, or other similar regulatory requirements. Nonetheless, banks that do not comply with the CIP Rule may face supervisory action, particularly if the non-bank financial institution the bank has partnered with does not collect the customer's identifying information directly from the customer, as required by the CIP Rule.

This RFI will inform FinCEN's understanding in this area and assist FinCEN in evaluating the risks, benefits, and potential safeguards related to certain CIP Rule requirements applicable to banks. Specifically, FinCEN is seeking input from banks and other interested parties regarding the CIP Rule's SSN collection requirement, including potentially allowing banks to collect partial SSN information from the customer and using a third-party source to collect the full SSN. Partial SSN collection refers to the practice where a bank may collect a certain part of the SSN from individuals who are the customers (*e.g.,* last four digits of an individual's SSN), and then obtain the full SSN from a reputable third-party service provider.

II. Request for Information Overview

FinCEN is aware of public interest by banks, trade associations, and Congress about the SSN collection requirement.[15] In particular, there has been expressed interest in permitting banks to collect a partial SSN while also permitting the use of reputable third-party sources to obtain the full SSN prior to account opening. FinCEN is interested in comments from the public on whether permitting partial SSN collection by a bank prior to account opening may promote, with appropriate safeguards, increased accessibility to financial services for a broader population of individuals. As noted earlier, this practice is currently not permissible under the CIP Rule, except for the previously described exception for credit card accounts.[16]

FinCEN recognizes the expansion of additional tools, sources, and methods available to banks since the initial adoption of the CIP Rule in 2003 to collect and verify customer identifying information, for example the emergence of new identity sources such as state mobile driver's licenses.[17] FinCEN also

TIN. In such cases, instead of obtaining a TIN from a customer prior to opening an account, the bank's CIP may include procedures for opening an account for a customer (including an individual) that has applied for, but has not received, a TIN. *See* 31 CFR 1020.220(a)(2)(i)(B).

[9] 68 FR 25103, at p.103 (May 9, 2003) (codified at 31 CFR 1020.220(a)(4)), *available at https://www.federalregister.gov/citation/68-FR-25103.*

[10] *Id.* at p.113.

[11] *Id.* at p.116.

[12] *Id.* at p. 103. *See also* H.R. Rep. No. 107–250, pt. 1, at 63 (2001).

[13] *Id.* at p. 105.

[14] FinCEN and the Agencies have previously issued interagency guidance on the applicability of the CIP Rule to prepaid cards. The guidance clarifies that certain prepaid cards issued by a bank should be subject to the bank's CIP, including when a bank issues prepaid cards under arrangements with third-party program managers that sell, distribute, promote, or market the prepaid cards issued by the bank. *See Interagency Guidance to Issuing Banks on Applying Customer Identification Program* (Mar. 21, 2016), *available at https://fincen.gov/sites/default/files/shared/InterAgency Guidance20160318.pdf.*

[15] *See* Ranking Member Congresswoman Maxine Waters of the U.S. House Committee on Financial Services letter to FinCEN and the Agencies (Sept. 7, 2023), *available at https://democrats-financialservices.house.gov/news/documentsingle.aspx?DocumentID=410778; see also* House Subcommittee on National Security, Illicit Finance, and International Financial Institutions Hearing Entitled: ''Oversight of the Financial Crimes Enforcement Network (FinCEN) and the Office of Terrorism and Financial Intelligence (TFI)'' (Apr. 27, 2023), *available at https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=408719* (which entered into the Congressional Record a letter from the American FinTech Council to H. Das, Acting Director of FinCEN titled ''Comments Regarding Regulatory Clarity, CIP Rules, and Consumer Products'' (Apr. 3, 2023), *available at https://fintechcouncil.org/fincen-bnpl*); and House Subcommittee on National Security, Illicit Finance, and International Financial Institutions Hearing Entitled: ''Oversight of the Financial Crimes Enforcement Network (FinCEN) and then Office of Terrorism and Financial Intelligence (TFI)'' (Feb. 14, 2024), *available at https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=409139* (which had questions regarding TIN collection entered into the record).

[16] *See* 31 CFR 1020.220(a)(2)(i).

[17] *See* Department of Homeland Security, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Waiver for Mobile Driver's Licenses, 88 FR 60056 (Aug. 30, 2023), *available at https://www.federalregister.gov/d/2023-18582.*

recognizes there are, and will be, more available customer identifying attributes that banks may collect (*e.g.,* email address, geolocation, and internet protocol (IP) address location), some of which vary in accuracy and authenticity, but which could be used holistically as part of a banks' risk-based verification procedures under the CIP Rule.

Notwithstanding these advancements, FinCEN is aware of consumer fraud and protection concerns around permitting a bank to obtain the full SSN from a third-party service provider. For instance, by permitting a bank to collect only the last four digits of an SSN from a customer who is an individual, a bank may increase the ease and speed of identity theft, including synthetic identity fraud that can result in accounts opened without appropriate safeguards.[18] Additional risks may arise if there is inaccuracy when using a third-party source to obtain an individual's full SSN, which may lead to potential impediments to law enforcement investigative efforts in obtaining accurate customer identifying information. FinCEN also recognizes differing regulatory requirements for customer information required between banks and other entity types, which may not subject to the BSA and FinCEN's implementing regulations, may result in regulatory arbitrage and even allow for illicit finance activity risk to remain undetected in the U.S. financial system, particularly by entities not subject to suspicious activity reporting requirements pursuant to the BSA.[19]

This RFI seeks information and comment on the potential risks, benefits, and safeguards around banks collecting partial SSNs for U.S. individuals directly from the customer and subsequently using reputable third-party sources to obtain a full SSN prior to account opening. FinCEN is also gathering information about current industry practices regarding SSN collection. This RFI also seeks responses to specific questions below.

III. Suggested Topics for Commenters

To allow FinCEN to evaluate comments more effectively, FinCEN requests that, where possible, comments include any suggested use of FinCEN authorities, or changes to FinCEN regulations or guidance, including the nature of the requested change and supporting data or other information on impacts, costs, and benefits.

The following questions are intended to assist in the formulation of comments and are not intended to restrict what may be addressed by the public. Commenters may also address matters that do not appear in the questions below related to the CIP Rule's SSN collection requirement. FinCEN requests that, in addressing these questions, commenters identify issues in as much detail as possible and provide specific examples where appropriate. Commenters are requested to comment on some or all of the questions below and are encouraged to indicate in which area the comments are focused. FinCEN requests that commenters note their highest priorities in their response, along with an explanation of how or why certain suggestions have been prioritized, when possible.

1. Should banks be permitted to collect part or all of a customer's SSN for a U.S. individual from a third-party source prior to account opening? Should banks be permitted to collect other customer identifying information required by the CIP Rule from a third-party source?

2. If banks were permitted to collect partial SSN information from a customer in the case of a U.S. individual and subsequently use a reputable third-party source to obtain the full SSN prior to account opening:

a. What would be the risks and benefits of permitting this partial SSN collection practice for banks?

b. What safeguards would need to be in place? What impact would there be on a bank's policies, practices, and procedures?

c. What practices and procedures would banks use to obtain a customer's full SSN when a partial SSN is collected from the customer?

d. How would the collection of a partial SSN from the customer impact how a bank forms a reasonable belief of the customer's identity?

e. How would the reliance on third-party sources for SSN collection impact the adherence to CIP recordkeeping requirements, if at all?

f. What minimum due diligence processes would a bank typically conduct, or expect to conduct, before contracting with a third-party source for SSN collection? How do banks review and assess the capability, quality, and performance of the third-party source, including the accuracy and reliability of the full SSN collected by the third-party source?

g. What ongoing due diligence and monitoring would be conducted on the third-party source? How frequently would ongoing due diligence be conducted?

h. What measures could banks have in place to verify the accuracy of a full SSN retrieved from a third-party source?

i. How would existing third-party monitoring and due diligence processes be modified to ensure the privacy and security of customer data?

j. What would be the impact of allowing partial SSN collection with third-party validation in terms of identity theft-related safeguards for customers?

3. Regarding the current CIP Rule SSN collection requirement for banks to collect the full SSN for a U.S. individual directly from the customer prior to account opening:

a. What is the impact of the current requirement on banks and their customers to collect the full SSN directly from the customer?

b. Does the current SSN collection requirement impact a customer's ability to access financial products and services?

c. How does the current SSN collection requirement impact a bank's AML program? What type of changes to the SSN collection requirement would improve the risk-based nature of a financial institution's AML program?

d. What are the risks and benefits of collecting a full SSN directly from the customer? What safeguards are in place to protect SSN information?

e. Is there any impact on the SSN collection requirement from the method used by the customer to access a bank's products and services (*e.g.,* mobile application, third-party website, face-to-face)?

f. What factors and consideration may be necessary to identify, assess, and mitigate any risks associated with new technologies or innovative approaches to the SSN collection requirement?

g. Is there any impact on the SSN collection requirement related to geography? For example, how should the location of the customer be considered in terms of the SSN collection requirement?

h. Do certain financial products and services pose higher or lower levels of risk in terms of the SSN collection requirement? Are there certain products or services that are better placed for either full or partial SSN collection?

i. For banks registered to use an authoritative, government-affiliated source for verification, such as the Social Security Administration's

[18] *See* FinCEN, *Financial Trends Analysis: Identity-Related Suspicious Activity: 2021 Threats and Trends* (Jan. 2024), *available at https://www.fincen.gov/sites/files/shared/FTA_Identity_Final508.pdf* (which highlights the use of ''synthetic identity,'' a combination of real and fake customer identifying information, to exploit a financial institution's identity verification processes).

[19] *See* 31 CFR 1022.210(d)(1)(i)(A). Money services businesses, for example, have an AML Program requirement to verify customer identification, but are not subject to the CIP Rule.

electronic Consent Based SSN Verification (eCBSV) program, which typically requires customer consent prior to accessing this program, how would banks be able to use the eCBSV program if banks no longer obtained the full SSN from the customer?

4. Regarding current practices by parties not subject to the CIP Rule's SSN collection requirement (*i.e.,* non-banks) when using third-party sources for SSN collection:

a. What are the risks and benefits of using a third-party source for SSN collection?

b. What minimum due diligence processes does a non-bank typically conduct before contracting with a third-party source for SSN collection? How do non-banks review and assess the capability, quality, and performance of the third-party source, including the accuracy and reliability of the full SSN collected by the third-party source?

c. What ongoing due diligence and monitoring do non-banks conduct on the third-party source? How frequently is ongoing due diligence conducted?

d. What measures do non-banks have in place to verify the accuracy of a full SSN retrieved from a third-party source?

e. How do non-banks ensure the privacy and security of customer data when using a third-party source for SSN collection?

f. What authoritative or private sector third-party sources are generally used for obtaining SSNs?

g. What, if any, limitations and/or shortcomings have been identified in third-party sources used to obtain SSN information?

h. What is the typical timeframe from when a customer enters their partial TIN to the non-bank receiving the full SSN from the third-party source?

i. What types of processes or strategies may be employed by third-party sources to manage high volume and/or time-sensitive SSN collection requests?

j. How frequently do customers fail the third-party SSN collection? What process(es) can be applied in such instances?

k. Have there been expected or observed differences in the rate of fraud or suspicious activity when non-banks using a partial SSN collection process versus full SSN collection directly from a customer?

l. How frequently does the partial SSN provided by a customer match to more than one individual when submitted to a third-party source? What additional steps are taken in such a case?

m. When the customer provides a partial SSN, is the customer notified that the remaining digits of their SSN will be obtained from a third-party source? Are there instances when non-banks may display a full SSN to a customer who provided a partial SSN? How would non-banks address and mitigate identity theft-related risks in those instances?

5. Provide any publicly available studies or data points that demonstrate:

a. Customer behavior in seeking or avoiding access to financial products or services based on risks associated with a customer providing a full SSN, whether perceived or actual.

b. Accuracy and reliability of third-party sources from which SSN information could be acquired.

c. Impact on financial crime or other illicit finance activity risks when a customer is not required to provide a full SSN.

d. The benefits and risks for non-banks (*e.g.,* employers, retailers, financial service providers, and government agencies) and third-party service providers in obtaining a partial SSN from the customer and then using a third-party source to obtain the customer's full SSN.

6. Regarding current CIP practices of all financial institutions, both banks and non-banks:

a. What risks have been identified with the SSN collection requirement, and how have those risks been mitigated?

b. Do financial institutions use a combination of documentary and non-documentary methods to verify the identity of its customers, or do financial institutions rely solely on one of the two methods?

i. For financial institutions that do not rely on a combination of both methods, what is the rationale?

ii. For financial institutions that rely solely on non-documentary methods, what is the rationale and what information is collected to form a reasonable belief that it knows the true identity of the customer?

c. What are the variations to TIN collection and verification practices used by financial institutions?

d. Other than processes related to TIN collection and verification, what other means are used by financial institutions to collect and verify customer identifying information?

e. Describe the processes and technologies used by financial institutions when obtaining and verifying partial and/or full customer identifying information as it pertains to various delivery channels (such as telephonic, mobile, and point-of-sale).

f. Describe similarities and differences in the collection and verification practices by financial institutions between individuals who provide SSNs and legal entities that provide Employer Identification Numbers.

7. What are the competitive advantages and disadvantages between banks that are required to collect the full SSN from the customer and those non-banks that collect a partial SSN from the customer and then use a third-party source to obtain the customer's full SSN?

8. What types of products/services are impacted by differing regulatory requirements related to SSN collection?

Andrea M. Gacki,

Director, Financial Crimes Enforcement Network.

[FR Doc. 2024–06763 Filed 3–28–24; 8:45 am]

BILLING CODE 4810–02–P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Actions

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the names of one or more persons that have been placed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of these persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

DATES: See **SUPPLEMENTARY INFORMATION** section for applicable dates.

FOR FURTHER INFORMATION CONTACT: OFAC: Bradley T. Smith, Director, tel.: 202–622–2490; Associate Director for Global Targeting, tel.: 202–622–2420; Assistant Director for Licensing, tel.: 202–622–2480; Assistant Director for Regulatory Affairs, tel.: 202–622–4855; or the Assistant Director Compliance, tel.: 202–622–2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website (*https://www.treasury.gov/ofac*).

Notice of OFAC Action(s)

On March 26, 2024, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following persons are