May 24, 2024

Andrea M. Gacki
Director
Financial Crimes Enforcement Network
Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

Re: Request for Information and Comment on Customer Identification Program Rule Taxpayer Identification Number Collection Requirement
(Docket Number FINCEN-2024-0009)

The Financial Technology Association (FTA) appreciates the opportunity to respond to this Request for Information (RFI) concerning the Customer Identification Program (CIP) rule's Taxpayer Identification Number (TIN) collection requirement issued by the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN). FTA applauds FinCEN's proactive efforts to modernize its regulatory frameworks, including identifying and revising any outdated, redundant, or ineffective regulations and guidance related to its anti-money laundering and countering the financing of terrorism (AML/CFT) framework, as required under the Anti-Money Laundering Act of 2020. In the meantime, FTA strongly urges FinCEN to ensure that regulation remains technology neutral and does not permanently alter the competitive landscape by deterring consumer use of digital providers and channels pending rule modernization. For this reason—and as detailed below—immediate exceptive relief is necessary given FinCEN's current interpretation of CIP Rule requirements.

FTA is a nonprofit trade organization representing leading technology-centered financial services (fintech) companies. FTA members take our compliance obligations seriously and believe that technology can significantly improve the capabilities of industry and the government to identify and counter bad actors. We welcome the opportunity to engage with FinCEN on the critically important topic of modernizing U.S. AML/CFT regulations to ensure the efficiency and effectiveness of the overall regime.

In light of the rapid advancement of financial technologies and services, it is crucial that the CIP Rule be modernized to keep pace with innovation, data privacy enhancement, consumer preference accommodation, and the effective prevention, detection, and reporting of suspicious financial activity. This is particularly relevant in the context of bank-fintech partnerships, which have considerably broadened the range of accessible financial services, enhancing credit access and

diversifying payments solutions. The digital transformation of banking platforms, the diversification of financial products, and the increased collaboration of banks with non-bank financial entities have reshaped customer interactions and service delivery. These changes demand a dynamic regulatory framework that accommodates innovative products and adapts to digital methods of account opening.

To this end, since its finalization in 2003, under The USA PATRIOT Act, the CIP Rule has mandated that financial institutions subject to the rule collect and verify identifying information for individuals opening accounts,[1] including, at a minimum, collecting a U.S. Tax Identification Number (TIN)[2] prior to opening an account, for example a Social Security Number (SSN), an Individual Taxpayer Identification Number (ITIN), or an Employer Identification Number (EIN). Originally, the rule was designed for traditional, in-person account openings—a context in which customers typically visited banks to initiate their financial relationships. However, the regulation further recognized that not-in-person engagements may require different requirements, as is the case with credit card openings. Indeed, as the financial landscape increasingly adopts a digital-first approach, there is growing consensus that the rule needs to be modernized to reflect current realities and challenges, including by enhancing data security to avoid the creation of honeypots of sensitive information and transitioning away from a SSN-based identification system.[3]

In practice, banking regulators have recognized these dynamics and accepted interpretations of the law that permit variations in SSN collection, such as collecting only the last four digits of a SSN directly from the customer and obtaining the remainder from trusted third-party sources, a method referred to as the "SSN Combined Collection Method." Such methods, commonly used by providers not subject to the CIP Rule, do not pose additional risks for money laundering or terrorist financing activities compared to the full collection of SSNs.[4] Industry participants have adopted these methods, underscoring that any sudden departure from this practice will disrupt the market—likely permanently given shifts in consumer behavior—and harm consumer access to digitally-driven financial services.

However, FinCEN's recent RFI marks a significant shift away from recognizing this accepted practice by proposing the collection of full SSNs at account opening. This change contradicts the legal directions previously provided to some entities and introduces undue risk and friction into the account verification process. It will also deter consumers from pursuing particular financial

[1] 68 Fed. Reg. 25090 (May 9, 2003).
[2] See Section 6109 of the Internal Revenue Code (26 USC 6109) and the IRS regulations implementing that section (26 CFR Part 301.6109-1).
[3] The Better Identity Coalition (2018) *Better Identity in America: A Blueprint for Policymakers*. Available at: https://docs.house.gov/meetings/BA/BA00/20190912/109912/HHRG-116-BA00-Wstate-GrantJ-20190912-SD001.pdf.
[4] Customer Identification Program Rule Exemption Request for [OpSub], an Operating Subsidiary of [Bank], OCC Interpretive Letter #1175 at 1 (Nov. 16, 2020), https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1175.pdf.

services and products due to distrust of providing the full-nine in a digital channel, as well as deter providers from developing technologies capable of enhancing ID verification without relying heavily on analog identifiers like the SSN.[5]

Given the substantial risks posed by this interpretation of the CIP Rule, it is crucial to grant immediate exceptive relief for entities relying on the SSN Combined Collection Method. Following such joint-agency relief, which should be viewed as a temporary measure, FinCEN should collaborate with banking regulators to modernize the CIP Rule, enhance clarity, and reflect rapid advancements in digital banking, including the emergence of innovative identity verification technologies. Eliminating the requirement to collect the full nine-digit SSNs from customers at account opening would align with data minimization best practices and enhance overall data security. The same principles of data minimization and data security that apply to SSNs should also extend to ITINs. By adopting these principles, financial institutions can enhance the protection of sensitive customer information.

FTA accordingly provides the following feedback and recommendations regarding the CIP Rule:

- FinCEN and the federal banking agencies should grant immediate exceptive relief from the requirement to collect full nine-digit SSNs at account opening, explicitly accepting the Combined Collection Method. This approach would align with digital realities of the marketplace, enhance data security, and ensure that competition is not permanently impacted pending a rulemaking to modernize the CIP Rule.
- Second, if exceptive relief is not granted broadly, then FinCEN and the federal banking agencies should implement immediate carve-outs for certain consumer products and Buy Now Pay Later (BNPL) services, reflecting their lower risk profile, similarity to previously excepted products, such as credit cards, and unique operational characteristics.
- Finally, FinCEN should modernize the CIP Rule through a joint-agency rulemaking that enhances clarity and adopts a principles-based approach encouraging innovation and collaboration.

[5] Financial Technology Association (FTA) (2024) Unpacking the Customer Identification Program (CIP) Rule and Its Implications for Financial Inclusion. Available at: https://www.ftassociation.org/unpacking-the-customer-identification-program-cip-rule-and-its-implications-for-financial-inclusion/.

I. *FinCEN should grant immediate exceptive relief from "full-nine" SSN digit collection, accepting the practice of obtaining only the last four digits directly from the customer and the remainder from trusted third-party identification partners, in order to enhance data security, ensure the status quo of the marketplace pending a rulemaking, and align with consumer preferences.*

As noted above, exceptive relief is necessary as a temporary measure before modernizing the CIP Rule to prevent regulations disproportionately favoring certain providers and products, which could permanently impede and impact the competitive marketplace. This relief would also be consistent with ensuring that regulation remains technology neutral. Many providers have historically relied on the Combined Collection Method—collecting only the last four digits of a SSN directly from the customer and obtaining the remainder from third-party sources, often with tacit or explicit regulator approval—and now face a competitive disadvantage given the current interpretation of the CIP Rule. Given that this method, involving partial SSN collection and third-party verification, has effectively met key regulatory objectives, FinCEN should grant broad, immediate exceptive relief to ensure fairness and prevent undue disadvantage in the marketplace pending a new rulemaking.

A. The Combined Collection Method not only enhances data security and privacy, but also best satisfies consumer preferences.

The Combined Collection Method adheres to data minimization best practices, significantly enhancing privacy and reducing the volume of sensitive personal information processed or held by institutions. Particularly in digital banking, the impracticality and increased privacy risks of requiring full SSNs during onboarding in remote financial transactions are evident. As digital interactions proliferate, the risks associated with the electronic collection of the "full-nine" SSN are magnified, potentially exposing consumers to heightened risks of identity theft. Thus, limiting SSN collection to only the last four digits substantially mitigates these risks, aligning with data protection best practices and the safeguarding of consumer privacy. It further allows financial institutions more freedom and flexibility to store this information in a secure manner, while still providing law enforcement with enough information to locate subjects under investigation.

The original CIP Rule was crafted with an understanding that collection of the "full-nine" could become unnecessary and potentially harmful in non-physical settings. The Rule states:

> Treasury and the Agencies are mindful of the legislative history of section 326, which indicates that Congress expected the regulations implementing this section to be appropriately tailored for accounts opened in situations **where the account holder is not physically present at the financial institution and that the**

> **regulations should not impose requirements that are burdensome, prohibitively expensive, or impractical**.[6] (emphasis added)

This philosophy supports extending exceptive relief to digital financial services on the same grounds as for credit card accounts. Indeed, FinCEN has acknowledged the appropriateness of the Combined Collection Method, stating that "Treasury and the Agencies recognize that these practices have produced an efficient and effective means of extending credit with little risk that the lender does not know the identity of the borrower."[7] This precedent supports extending similar exceptions to digital financial services, especially pending a rulemaking effort to modernize the CIP Rule.

Consumer preferences also strongly support the need for exceptive relief; since 2003, the requirement for financial institutions to collect full SSNs has raised significant privacy concerns.[8] Requiring a consumer to provide a full SSN in a digital context is antithetical to common practice and will increase privacy or illicit activity concerns, impacting marketplace dynamics and competitiveness, as well as hindering access to products offered through digital channels.[9] Put simply, many consumers would be surprised, concerned, and deterred by a prompt requiring entry of their full SSN.[10]

To be sure, consumer concern with providing full SSNs is well-founded. In 2017, identity fraud in the U.S. resulted in losses totaling $16.8 billion, during a year marked by a staggering 44.7% increase in data breaches, according to the Identity Theft Resource Center.[11] These breaches exposed nearly 179 million records containing personal information, underscoring the critical need for stringent data protection measures that align with the realities of modern digital financial interactions and consumer expectations. Immediate exceptive relief to the "full-nine" interpretation of the CIP Rule is therefore necessary and appropriate pending modernization through rulemaking.

---

[6] 68 FR 25090, 25097; Referencing H.R. Rep. No. 107–250, pt. 1, at 63 (2001).
[7] 68 Fed. Reg. at 25090.
[8] 68 Fed. Reg. at 25090, 25091, 25098.
[9] 68 Fed. Reg. at 25090, 25091.
[10] Hon. Waters, M. (2023) "Ranking Member Waters Asks U.S. Financial Agencies to Examine Customer Identification Program to Modernize Rules, Ensure Consumer Protection and Combat Bad Actors." Available at: https://democrats-financialservices.house.gov/uploadedfiles/09.06.2023_cip_prog.pdf. ("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.")
[11] The Better Identity Coalition, 2018.

B. Trusted third-party identification partners fit within existing risk management frameworks.

Trusted third-party identification partners play a crucial role within existing risk management frameworks established by federal banking agencies. These frameworks recognize that banks and financial institutions routinely rely on third parties for essential data solutions and identity services.[12] Such partnerships are not merely supplemental; they are integral to the operational strategies of these institutions, aiming to ensure consistency and enhance compliance efforts.

Leveraging third-party services offers significant advantages to banking organizations. It provides expedited access to advanced technologies, specialized human capital and solutions, broader delivery channels, diverse financial products, and expanded market access.[13] These relationships enable institutions to navigate the complex landscape of financial services with greater agility and innovation, ensuring that they remain competitive and responsive to market demands. Such relationships further enhance and improve regulatory compliance, including with respect to identity verification.

As a point of reference, the IRS incorporates trusted third-party services in operationalizing its Income Verification Express Service (IVES) program.[14] IVES allows authorized lenders to access a taxpayer's tax records for income verification purposes, with such access commonly facilitated by trusted third-party providers. Moreover, Money Services Businesses (MSBs) and other entities generally not covered by the CIP Rule routinely engage third-party vendors to safely verify identities, while adhering to the strict principles of data security, privacy, and minimization.

These third-party relationships enable providers to leverage innovative technologies for identity verification without the risk of creating multiple honeypots of customer information at each institution.[15] The accuracy of identity verification by these third-party vendors often surpasses that of methods relying solely on consumer-provided full nine-digit SSNs;[16] given the inherent vulnerability of knowledge-based authenticators (KBA), such as the full-nine SSN, experts across government and the private sector are encouraging use of multifactor authentication (MFA) that

[12] 88 Fed. Reg. 37920 (June 9, 2023).
[13] 88 Fed. Reg. at 37920, 37921.
[14] Internal Revenue Service (IRS) (18-Mar-2024) *IVES enrollment procedures*. Available at: https://www.irs.gov/individuals/ives-enrollment-procedures (Accessed: May 7, 2024).
[15] Financial Technology Association (FTA), 2024
[16] See generally Waters, 2023 ("Such tools [offered by third-party vendors] 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.")

goes beyond KBA—this is where third-party vendors are leading the charge and sound policy should be facilitating further development.[17]

II. Absent broader exceptive relief, consumer lending and BNPL products should be specifically carved out from "full-nine" SSN collection requirements and allowed to use the Combined Collection Method.

In the event that FinCEN does not grant broad exceptive relief for all digital financial products, it should do so for those consumer products most analogous to already excepted categories. Specifically, consumer lending and Buy Now, Pay Later (BNPL) products, with their inherently lower money laundering risks and operational similarities to credit card accounts, warrant consistent regulatory treatment under the CIP Rule. Subjecting these products, which directly compete with credit cards, to more stringent SSN collection requirements places them at an unfair competitive disadvantage.

The formal adoption of the CIP Rule reflects Congress's intent for regulations under Section 326 to be "appropriately tailored" to the realities of different financial products.[18] For credit card accounts, Treasury and the Agencies recognized that requiring the collection of full SSNs would "alter the manner in which they do business by requiring them to gather additional information beyond that which they currently obtain directly from a customer who opens an account at the point of sale or by telephone."[19] This understanding led to an exception in the final rule for credit card accounts, allowing banks to collect some information directly from the customer and the remainder from a trusted third-party source before extending credit. This approach has been acknowledged by Treasury and the Agencies as "an efficient and effective means of extending credit with little risk that the lender does not know the identity of the borrower."[20]

Similarly, for BNPL and other consumer credit products, requiring customers to provide all nine digits of the SSN for each transaction is not only unreasonable, but also impractical, particularly given the frequent nature of BNPL transactions. Therefore, extending similar exceptions to these products, as has been done with credit card accounts, is both warranted and necessary to maintain a level playing field within the financial industry.

---

[17] See Bushwick, S. (2021) "Social Security Numbers Aren't Secure: What Should We Use Instead?," Scientific American, 24 September. Available at: https://www.scientificamerican.com/article/social-security-numbers-arent-secure-what-should-we-use-instead/, ("[T]he more secure [MFA] approach is gradually becoming more popular . . . the U.S. federal government, financial industry and tech companies are beginning to require multiple layers of authentication."

[18] 68 Fed. Reg. at 25097.

[19] 68 Fed. Reg. at 25097.

[20] 68 Fed. Reg. at 25090, 25097.

III. Following issuance of exceptive relief, FinCEN should initiate a joint-agency rulemaking process to modernize the CIP Rule, shifting to a more principles-based approach to encourage innovation and collaboration.

Technological advancements and new data sources have transformed the compliance landscape since the original CIP Rule was established. Initiatives such as the recent FinCEN and FDIC techsprint and the 2023 NIST webinar series on Digital Identity Guidelines[21] underscore the pivotal role of innovation in customer identification solutions for remote onboarding,[22] including current advancements in identity proofing such as the use of digital identity credentials. The 2018 joint statement issued by FinCEN and the federal banking agencies reinforced the importance of—and encouraged—banks to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to combating money laundering, terrorist financing, and other illicit financial activities.[23] These efforts promote a regulatory environment that fosters innovation and encourages institutions to find new ways of using existing tools, or adopt new technologies, to develop effective AML/CFT compliance programs.

With recent technology innovations, we now have access to better tools to share, store and verify personal data. Decentralized Identifiers (DIDs), for example, are a new type of identifier that enables verifiable digital identity. A DID in the most simplistic sense, is a unique online identifier. Verifiable Credentials (VCs) are designed to represent claims about the subjects of DIDs, such as an individual or entity. They provide a standard way to express physical credentials in an online presentation in a way that is cryptographically secure, privacy respecting, and machine verifiable. VCs effectively mirror traditional photo identity and evidence proof documents, but offer less opportunity for tampering and identity theft, when issued by an authoritative source. DIDs and VCs provide a novel solution to fulfill compliance obligations in remote onboarding scenarios, improving on traditional methods employed today by financial institutions.

Despite the availability of new technologies, digital identity is not widely adopted by financial institutions because of the lack of guidance regarding how to deploy these technologies to meet traditional onboarding requirements, such as CIP. For example, there is a NIST project interested in proving-out remote presentation of mDL for accessing financial services. It offers a unique ability to prove the increased assurance levels of digital identity documents from direct sources, such as the state DMVs, and demonstrates how regulatory agencies continue to explore the benefits of this new technology; unfortunately, regulators are yet to release any substantial guidance to the industry on the appropriate application of digital identity for remote onboarding.

---

[21] National Institute of Standards and Technology (2023) "Digital Identity Guidelines Webinar Series," 16 March. Available at: https://www.nccoe.nist.gov/digital-identity-guidelines-webinar-series.

[22] FinCEN, 2022.

[23] *Treasury's FinCEN and Federal Banking Agencies Issue Joint Statement Encouraging Innovative Industry Approaches to AML Compliance* (2018) *U.S. Department of the Treasury*. Available at: https://home.treasury.gov/news/press-releases/sm562.

Interagency support for digital identity ensures that emerging standards for digital identity documents, verifiable credentials, and identity wallets protect the rights of consumers and ensures consistent application of this new technology, while realizing the potential for more efficient and effective online identity proofing. Additionally, this shift towards adoption of new technologies and approaches, including allowing institutions to utilize trustworthy third-party partners, can advance more secure and accurate identification verification. This will enhance customer convenience and security, while also promoting broader financial access by facilitating customer onboarding. Acting Comptroller of the Currency Michael J. Hsu has emphasized the importance of exploring innovative identity verification methods, such as accepting consular identification cards and municipal IDs, to help integrate new Americans into the financial system. This promotes a "risk-based approach to customer due diligence, rather than mak[ing] broad-based decisions affecting whole categories or classes of customers when provisioning access to services, capital, and credit."[24]

Recent initiatives, such as the FDIC and FinCEN digital identity tech sprint[25] and the 2023 NIST webinar series on Digital Identity Guidelines[26] demonstrate the urgent need to adapt the CIP Rule to technological advancements and dynamic market conditions.[27] These efforts highlight the rapid innovation in identity verification, which is better supported by principles-based frameworks rather than prescriptive rules.

For these reasons, FinCEN and the federal banking agencies should pursue a rulemaking to modernize the CIP Rule along the following objectives:

- Actively seek input from financial institutions, fintech companies and digital identity technology companies on opportunities to adapt the CIP Rule to promote and support the use of new innovative technologies to meet traditional compliance obligations.
- Encourage financial institutions to experiment with new approaches to customer identification and verification through official guidance.
- Cultivate a collaborative environment that allows regulators to stay informed and engaged with emerging technologies and methodologies used for identity verification.
- Move away from legacy KBA approaches to more dynamic multi-factor approaches that comport with data minimization principles, safeguard consumer privacy, and enhance accuracy.

[24] Acting Comptroller of the Currency Michael J. Hsu (2024) *Remarks for the Financial Literacy and Education Commission's Public Meeting Meeting the Needs of New Americans: Creating Opportunity*, Office of the Comptroller of the Currency (OCC). Available at: https://www.occ.gov/news-issuances/speeches/2024/pub-speech-2024-40.pdf.
[25] FinCEN (2022) FDIC FinCEN Digital Identity Tech Sprint - Key Takeaways and Solution Summaries. Available at: https://www.fincen.gov/news/news-releases/fdic-fincen-digital-identity-tech-sprint-key-takeaways-and-solution-summaries.
[26] National Institute of Standards and Technology (2023) "Digital Identity Guidelines Webinar Series," 16 March. Available at: https://www.nccoe.nist.gov/digital-identity-guidelines-webinar-series.
[27] Klein, A. (2024). "Comments on FinCEN's proposed changes to customer identification rules." Available at: https://www.brookings.edu/articles/comments-on-fincens-proposed-changes-to-customer-identification-rules/.

* * *

FTA appreciates the opportunity to provide feedback on CIP Rule modernization and the need for immediate exceptive relief to current rule interpretations. We share FinCEN's goal of advancing a safe and secure financial system, and modernizing AML/CFT regulations to account for innovative technology and developments, and would welcome opportunities to assist the bureau as it moves forward with these efforts.

Sincerely,

Penny Lee
President and Chief Executive Officer
Financial Technology Association