BANK POLICY INSTITUTE

November 13, 2018

Via Electronic Mail

Financial Crimes Enforcement Network
Attn: Policy Division
P.O. Box 39
Vienna, VA 22183

Re: Proposal to Renew Rule re Customer Identification Programs of Banks and Other Financial Institutions (Docket No. FINCEN–2018–0013; OMB Number 1506-0026)

Ladies and Gentlemen:

The Bank Policy Institute[1] appreciates the opportunity to respond to the notice and request for comment (referred to herein as the "proposal") issued by the Financial Crimes Enforcement Network of the U.S. Department of the Treasury ("FinCEN") to renew without change its rule prescribing the requirements for Customer Identification Programs ("CIPs") for banks.[2] We are committed to assisting FinCEN's efforts to detect and prevent money laundering and the financing of terrorism, and thus strongly support the fundamental principal of the rule that an effective CIP is an essential element of a bank's overall due diligence program. We also support the risk-based approach contemplated under the current rule, which provides for a CIP in each case that is appropriate given a bank's size and type of business. And we appreciate FinCEN's attempt in the rule "to strike an appropriate balance between flexibility and detailed guidance by allowing a bank broad latitude to design and implement a CIP that is tailored to its particular business practices while providing a framework of minimum standards for identifying each customer, as the [statute] mandates."[3] Each of these components of the existing rule serve important and effective policy goals, and we strongly support their continuation.

At the same time, we believe FinCEN's current exercise to review and renew the CIP rule presents an important opportunity to modernize other aspects of the current framework. In particular, given the rapid pace of development of financial products, services, and technologies, giving institutions a greater degree of flexibility around

---

1 The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

2 Our comments focus on the regulation applicable to banks, savings associations, credit unions, and certain non-Federally regulated banks (hereinafter "banks"), currently codified at 31 C.F.R. § 1020.220.

3 68 Fed. Reg. 25090, 25095 (May 9, 2003).

key parts of the rule (e.g., as to which customer information may be collected) would not only better reflect today's marketplace realities, but would also render the CIP rule more effective in achieving the intent behind the statutory provision mandating issuance of the rule: facilitating the prevention, detection, and prosecution of international money laundering and the financing of terrorism. For similar reasons, we believe that the CIP rule should allow for reliance, in appropriate circumstances, on a broader array of third parties to assist in performing CIP procedures. To those ends, this letter offers concrete ideas for improvement of the CIP framework along these lines.

Our comments on the proposal are organized as follows: Part I of this letter sets forth an executive summary of our comments; Part II provides historical background on the statutory requirement in Section 326 of the USA PATRIOT ACT (codified as 31 U.S.C. § 5318(l)) and the regulatory history of the CIP rule; Part III addresses the need for a greater degree of flexibility in the CIP rule; and Part IV addresses our comments on FinCEN's estimate of the burden of this collection on subject institutions.

I. Executive Summary

- Considerations that informed the statutory requirement as originally enacted, as well as the implementing regulation as originally adopted—including comments urging Treasury to allow banks greater flexibility in light of issues related to, among other things, consumer privacy and reliance on third parties—remain relevant today and demonstrate the need for flexibility.

- In light of the rapidly changing landscape of financial services and innovations in technology, FinCEN should revise the rule, through notice and comment, to provide institutions with more flexibility to adapt their CIP to reflect and take advantage of current and future innovations in identifying their customers—notably the ability to secure customer information from other trusted and secure sources for a broader set of account openings.

- The proposal underestimates the actual collection burden and does not consider compliance costs.

II. Considerations that informed the statutory requirement as originally enacted, as well as the implementing regulation as originally adopted—including comments urging Treasury to allow banks greater flexibility in light of issues related to, among other things, consumer privacy and reliance on third parties—remain relevant today and demonstrate the need for flexibility.

Section 326 of the USA PATRIOT Act amended the Bank Secrecy Act[4] to require the Secretary of the Treasury[5] to issue regulations prescribing CIPs for financial institutions that must, at a minimum, require financial institutions to implement (and customers, after being given adequate notice, to comply with) reasonable procedures for: (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.[6] Consistent with the statutory language, the congressional record of both the House of Representatives and the Senate emphasize that the minimum standards to be prescribed to give effect to section 326 should be "reasonable procedures."[7] And, the adopting release for the CIP rule notes that "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

---

4 31 U.S.C. § 5311 et seq.

5 This authority was delegated to the Director of FinCEN.

6 Section 326 was codified as 31 U.S.C. § 5318(l).

7 See 147 Cong. Rec. S10990-02 (Oct. 25, 2001); 147 Cong. Rec. H7159-03 (Oct. 23, 2001).

tailored...."[8] The adopting release also notes the importance of "strik[ing] an appropriate balance between flexibility and detailed guidance by allowing a bank broad latitude to design and implement a CIP that is tailored to its particular business practices while providing a framework of minimum standards for identifying each customer, as the Act mandates."[9]

In response to its original proposal in 2002, Treasury received comments that remain relevant, and are perhaps even more significant, today. Specifically, Treasury received comments on, among other issues, (i) consumer privacy, (ii) the requirement to obtain a customer's physical address, and (iii) reliance on third parties. With respect to consumer privacy, even fifteen years ago, individual commenters expressed concern that the requirement to obtain social security numbers "would expose them to an added risk of identity theft"[10] and institutions within the scope of the proposal "urged that banks be given the discretion to collect identifying information, other than social security numbers, when appropriate in light of consumer privacy and security concerns."[11] Similarly, with respect to the requirement to obtain a physical address, "most commenters" at the time urged Treasury to eliminate the requirement that the customer provide a physical address, noting that "requiring the customer to provide a physical address will discourage the provision of financial services to the underbanked and will prevent a victim of identity theft from using an alternative to an unsecured home mailbox."[12] With respect to reliance on third parties, commenters requested that "banks be given greater flexibility ... and urged that banks be permitted to rely on identification and verification of customers performed by a third party."[13]

Treasury considered these comments and determined to grant a modicum of relief in the context of credit card accounts and permit a very limited degree of reliance in other contexts.[14] As to the former, recognizing the unique nature of credit card operations and that requiring banks to collect identifying information from a customer prior to opening a credit card account "is likely to alter the manner in which they do business,"[15] Treasury permitted banks to secure identifying information, including social security numbers, from a third-party source.[16] Regarding reliance on third parties more generally, Treasury allowed banks to rely on a third party's performance of CIP, but only in limited circumstances: when (1) reasonable, (2) the third party is a financial institution that is subject to a CIP rule and has a Federal functional regulator, (3) the customer has a formal banking or business relationship with the other financial institution, and (4) the other financial institution annually certifies that it has implemented the bank's AML program and that it will perform the bank's CIP.[17] Treasury maintained the requirement to obtain a physical address, but, in an attempt to address the needs of the unbanked population, allowed an individual customer to use

---

8 68 Fed. Reg. 25090, 25097.

9 68 Fed. Reg. 25090, 25095.

10 68 Fed. Reg. 25090, 25091.

11 68 Fed. Reg. 25090, 25098.

12 68 Fed. Reg. 25090, 25097.

13 68 Fed. Reg. 25090, 25091.

14 31 C.F.R. § 1020.220(a)(2)(i)(C) and (a)(6).

15 68 Fed. Reg. 25090, 25097.

16 "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. Therefore, Treasury and the Agencies have included an exception in the final rule for credit card accounts only, which would allow a bank broader latitude to obtain some information from the customer opening the credit card account, and the remaining information from a third party source...." 68 Fed. Reg. 25090, 25097 (emphasis added).

17 *See* 31 C.F.R. § 1020.220(a)(6).

the residential or business address of a next of kin or another contact individual. This flexibility, while welcome, did not address, among other things, concerns with identity theft.

As discussed in greater detail in our comments that follow, we believe that the comments and considerations that led Treasury to provide limited allowances related to credit card accounts, reliance on third parties, and customer address, as well as significant additional considerations, weigh in favor of FinCEN revisiting the CIP rule with a view to affording banks even greater flexibility. The relief provided as to credit card accounts—"situations where the account holder is not physically present at the financial institution" in order to more appropriately accommodate "the manner in which [subject financial institutions] do business"—should be extended to a broader array of accounts in light of the current and rapidly changing methods by which customers interface with their banks and third parties. Indeed, we believe that doing so would give appropriate weight to the statutory factors Congress directed the Secretary of the Treasury to consider when issuing regulations to implement section 326: (1) various types of accounts maintained by various types of financial institutions, (2) various methods of opening accounts, and (3) various types of identifying information available. Similarly, Treasury's allowance for limited reliance on third parties should be extended and expanded to permit banks to rely on a broader array of third parties in appropriate circumstances.

III. In light of the rapidly changing landscape of financial services and innovations in technology, FinCEN should revise the rule to reflect a flexible approach capable of accommodating future innovation.

As technology and customer preferences continue to adapt in response to significant innovations, it is difficult—if not impossible—to predict accurately what the business environment for financial institutions will look like even five or ten years down the road. Regardless, concerns regarding the original CIP proposal, including with consumer privacy and the need for a flexible approach that is capable of accommodating appropriate technological innovations (either from within a financial institution itself or through partnerships with third parties) are highly relevant today. We believe it is important to consider how the existing rule can be reframed to allow financial technologies and innovations to be used to enable more efficient and reliable collection processes, including with respect to underbanked populations. Because the statute specifically directs the Secretary of the Treasury to consider certain factors in prescribing regulations to implement section 326, we address the two factors we believe should be revisited by FinCEN in light of the current and rapidly changing environment in which financial institutions operate before renewing the current CIP rule without change; namely, various methods of opening accounts and various types of identifying information available.

A. Various Methods of Opening Accounts: Banks Should Be Afforded Flexibility under the Rule to Secure Customer Information from Other Trusted and Secure Sources for a Broader Set of Account Openings

Gone are the days in which the vast majority of bank customers visited their local brick-and-mortar branch to meet with bank representatives to address their banking needs. Customers now expect to conduct their financial transactions using the quickest, securest, and most efficient means available—often using mobile channels and new financial technologies. Importantly, customers have often already provided identifying information to reliable third parties (or those reliable third parties have obtained identifying information) that can help facilitate that outcome if banks were afforded the flexibility under the CIP rule to more broadly rely on information secured from reliable third parties. The CIP rule was promulgated in very different times—before much of today's innovative financial technology existed—and reflects means of collecting and verifying customer information that are quickly becoming not only outdated but impracticable. Indeed, as to virtually all types of accounts offered by banks today, there should be an acknowledgement that, in appropriate circumstances, "accounts [may be] opened in situations where the account holder is not physically present at the financial institution[,]"[18] and in these scenarios, not just in the case of

[18] 68 Fed. Reg. 25090, 25097.

credit card accounts, banks should be allowed the flexibility to secure identifying information from a reliable third-party source.

A concern not present fifteen years ago when the CIP rule was promulgated is the rapid expansion of new companies offering a variety of innovative financial products and services to consumers outside the prescriptive regulatory environment applicable to traditional banking organizations. These products and services, if offered by a bank, often would qualify as "accounts" within the meaning of the CIP rule.

Because these new financial services companies often are not within the scope of the CIP rule, they may pursue innovative ways of efficiently, securely, and effectively identifying their customers that banks do not have the flexibility to pursue under the CIP rule. As consumer demand for faster account opening periods via mobile applications or other avenues increases, greater demands are placed on banks to collect and process information quickly, but without sacrificing data quality or security. In such an environment, the prescriptive requirements of the CIP rule place banks subject to the rule at a competitive disadvantage relative to entities that offer substantially the same product or service but are not subject to the rule—potentially including, as discussed below, restricted use of more advanced technologies or means of procuring reliable information from other trusted and secure sources.

The proposal specifically requests comment on "ways to minimize the burden of collection on respondents, including through the use of automated collection techniques or other forms of information technology."[19] We believe that a more risk-based and less prescriptive approach to collecting CIP information would allow banks to rely, in appropriate circumstances, on a broader array of third parties to collect information on customer identity. The focus of the CIP rule should be on the end result—that the bank is able to form a reasonable belief that it knows the true identity of its customer. The CIP rule should afford banks greater flexibility in how they achieve this end result.

B. Various Types of Identifying Information: Technological Innovations in the Collection and Custody of Customer Information

Continuation of requirements promulgated 15 years ago—before the advent of mobile financial technologies—effectively limits a bank's ability to take advantage of certain available technology that can enable a bank to form a reasonable belief that it knows the true identity of its customer. For example, while the statute requires only the name and address of each customer, the CIP rule currently also requires: date of birth, physical address, and social security number or other identification number—each of which has its own specific and additional requirements that must be met to satisfy the rule. Requiring banks to collect and store this broad range of detailed information effectively limits their ability to pursue other, potentially more reliable and more secure means of forming a reasonable belief that they know the true identity of their customer. Technological innovations in this area are rapid and expansive and include such things as embedded cameras for biometric identity collection, use of block chain/distributed ledger technologies to verify identification data within the consumer's control, use of mobile identity and location information through mobile platforms to verify address information,[20] and other, as yet unknown, advances. The ability to utilize these types of innovative solutions in the CIP space would not only serve to satisfy customer convenience, but also enable stronger security and more efficient and reliable collection processes.

Furthermore, with respect to concerns with consumer data privacy, and the use of social security numbers specifically, alternatives FinCEN should consider including in any proposed revision of the CIP rule are (i) requiring only the last four digits of the social security number to be provided by the customer and allowing the remainder of the number to be obtained from other trusted and secure sources, and/or (ii) move away from the use of social

---

19 83 Fed. Reg. 46015 (Sept. 11, 2018) at 46015.

20 This would work, for example, by (1) comparing the name, address, email address and phone number provided by the customer to what is on file with the carrier, ostensibly to make it more difficult to steal or fabricate an identity, and (2) using the location of a mobile phone to verify that the phone is in a location that corresponds with the identity information provided.

security numbers for individuals altogether by permitting the use of other identifiers, including—as currently permitted for non-U.S. persons—identification card numbers (which for U.S. persons would include state-issued identification cards) and passport numbers, or other identification numbers that customers may be more inclined to provide in light of data security concerns. Banking organizations would then be afforded flexibility with respect to the information they obtain from customers, depending on the type of product and whether other identifying information may be required for other purposes (such as tax reporting on interest-bearing accounts).

Moreover, banking organizations themselves may not be best placed to create, implement and execute these innovative solutions in-house. Partnerships with third party providers of innovative technologies are therefore of critical importance, and it is vital that FinCEN expand the reliance provisions in the CIP rule to a broader array of third parties. Many new financial technology companies that presently do not satisfy the CIP rule's reliance requirements may be well placed to partner with banks to provide efficient, effective and secure means of collecting and verifying customer information—not only via technologies noted above, but through technologies developed in the future. Use of new technologies such as distributed ledgers may also afford innovative ways for financial institutions to maintain records of information obtained from or about a customer and potentially mitigate the risk of consumer data breaches. Unlike the days when photocopies of a customer's driver's license were kept in a locked file cabinet in a bank's central storage, information is now provided and maintained digitally, exposing the custodian of such information to exponentially increasing data security costs and potential liability. These data privacy concerns counsel strongly against renewal without change of record-keeping requirements, and in favor of a more flexible, risk-based approach. Likewise, use of biometric data (which remains always within the custody of the consumer) for identity verification would be less susceptible to falsification, breach, and other potential misuse. The proposal to renew the current CIP rule without change would not provide much needed regulatory flexibility to pursue better solutions in this area. The CIP rule should be revised to establish higher-level objectives and expand subject institutions' ability to innovate and/or engage a broader array of third parties to perform CIP.

IV. The proposal underestimates the actual collection burden and does not consider compliance costs.

The proposal also specifically requests comment on "the agency's estimate of the burden of the collection of information."[21] We believe that the estimate provided in the proposal—10 hours of annual record-keeping burden—is a gross underestimate of the actual collection burden, to say nothing of the costs of compliance.[22]

Thomson Reuters conducted a survey in 2017 entitled "KYC Compliance: the rising challenge for financial institutions," which collected data during the second quarter of 2017 (before FinCEN's customer due diligence rule became effective on May 11, 2018).[23] While the information reported in this study includes costs and other data on "know your customer" ("KYC") and customer due diligence ("CDD") processes more generally, it provides data points indicative of the rising compliance and business costs in this area, a portion of which inarguably are driven by currently required CIP processes. The survey found, based on information from respondents, that customer onboarding time increased 8 percent in 2017 and was expected to increase by another 12 percent in 2018.[24] Indeed, the survey reported that it takes, on average, 26 days to onboard a new client (with corporate customers claiming that on average it takes 32 days), and banks reported that they contact their clients on average four times during the

---

21 83 Fed. Reg. 46015 (Sept. 11, 2018) at 46015.

22 For additional information on resources devoted to BSA/AML compliance more generally, please refer to Bank Policy Institute, *Getting to Effectiveness – Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance* (Oct. 29, 2018), *available at*: https://bpi.com/wp-content/uploads/2018/10/BPI-AML-Sanctions-Study-vF.pdf.

23 Bank spending, staffing and other preparations in anticipation of the final compliance date for the new CDD rule likely accounts for some portion of the noted increases relative to 2016.

24 Thomson Reuters, *KYC Compliance: the rising challenge for financial institutions*, at 4.

onboarding process (eight times for corporate customers).[25] Financial institutions reported in this survey that changes in legislation and regulation remain the biggest driver of changes to KYC processes generally. The largest financial institutions reported that their average spending on KYC-related procedures increased from $142 million in 2016 to $150 million in 2017, with the number of employees working on KYC compliance rising from an average of 68 in 2016 to 307 in 2017—an increase of over 350 percent in one year.[26]

Aside from these significant and rising regulatory compliance costs, inefficient KYC processes can further result in costly real-world business consequences for banks. Indeed, 12 percent of corporate clients surveyed reported that they had changed banks as a result of KYC issues.[27] In response to these client experience issues, financial institutions are "looking to invest in external resources and third party solutions to help improve the efficiency and regulatory compliance of their CDD/KYC processes."[28] Data security and privacy concerns would necessarily inform and guide any such efforts with respect to consumer product offerings. These efforts to improve efficiency and manage client needs and expectations would be facilitated by allowing banks additional latitude to employ third party resources and other innovative solutions, as explained in greater detail above.

For the reasons discussed throughout this letter, we urge FinCEN to reconsider a more risk-based and less prescriptive approach to obtaining required customer information under the CIP rule to allow banks to accommodate rapidly changing customer preferences and financial technologies without sacrificing—and, indeed, potentially improving—the effectiveness of efforts to facilitate the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Accordingly, we request that a revised CIP rule be proposed for comment, including any necessary conforming changes across related Treasury regulations.

* * * * *

The Bank Policy Institute appreciates the opportunity to comment on the proposal. If you have any questions, please contact the undersigned by phone at 202-589-1935 or by email at *Angelena.Bradfield@bpi.com.*

Respectfully submitted,

Angelena Bradfield
Vice President, AML/BSA, Sanctions & Privacy
Bank Policy Institute

---

25 *Id.* As noted, the information reported in the study encompasses KYC and CDD more generally and is not limited to account opening.

26 *Id.*

27 *Id.*, at 6.

28 *Id.*