ORDER

ORDER granting an exemption for all accounts at all banks subject to the jurisdiction of the Board of Governors of the Federal Reserve System from a Customer Identification Program (CIP) Rule requirement implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l), related to a bank obtaining Taxpayer Identification Number (TIN) information from the customer. The exemption in this ORDER permits a bank to use an alternative collection method to obtain TIN information from a third-party rather than from the customer, provided that the bank otherwise complies with the CIP Rule, which requires written procedures that: (1) enable the bank to obtain TIN information prior to opening an account; (2) are based on the bank's assessment of the relevant risks; and (3) are risk-based for the purpose of verifying the identity of each customer to the extent reasonable and practicable, enabling the bank to form a reasonable belief that it knows the true identity of each customer.[1]

Issue Date: July 31, 2025

By ORDER, under the authority set forth in 31 C.F.R. § 1020.220(b) implementing section 326(a) of the USA PATRIOT Act, 31 U.S.C. § 5318(l)(5), the Board of Governors of the Federal Reserve System (Board), with the concurrence of the Financial Crimes Enforcement Network (FinCEN), hereby grants an exemption from a requirement of the CIP Rule implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l), in the circumstances specified below.[2] Specifically, this ORDER provides an exemption from the requirement for banks subject to the jurisdiction of the Board[3] to obtain TIN[4] information from the customer prior to opening an account in the situations discussed herein.[5] This ORDER permits banks, for all accounts[6] at all

[1] 31 C.F.R. § 1020.220(a)(1) and (2).

[2] *See* 12 C.F.R. §§ 208.63(b)(2) and 211.24(j)(2). FinCEN, the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) have also issued regulations implementing this section of the USA Patriot Act. *See* 31 C.F.R. § 1020.220 (FinCEN); 12 C.F.R. § 21.21(c)(2) (OCC); 12 C.F.R. § 326.8(b)(2) (FDIC); and 12 C.F.R. § 748.2(b)(2) (NCUA) (collectively with the Board's regulation, the CIP Rule).

[3] This ORDER is applicable to banks, and their subsidiaries, that are subject to the jurisdiction of the Board. This ORDER does not apply to banks not subject to the jurisdiction of the Board. On June 27, 2025, with the concurrence of FinCEN, the OCC, FDIC, and NCUA (each an "Agency" and collectively together with the Board the "Agencies") issued an order applicable to banks subject to their jurisdiction. *See* FinCEN Permits Banks to Use Alternative Collection Method for Obtaining TIN Information; FDIC: Agencies Issue Exemption Order to Customer Identification Program Requirements; OCC: Acting Comptroller of the Currency Issues Statement on Order Granting Exemption to Customer Identification Program; NCUA: Agencies Issue Exemption Order to Customer Identification Program Requirements.
The term "bank" is defined in regulations implementing the BSA, 31 C.F.R. § 1010.100(d), and includes each agent, agency, branch, or office within the United States of banks, savings associations, credit unions, and foreign banks.

[4] *See* 31 C.F.R. § 1020.220(a)(2)(i)(A)(4); *see also* 31 C.F.R. § 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.,* Social Security Number (SSN), individual taxpayer identification number (ITIN), or employer identification number (EIN)).

[5] Under the CIP Rule, a TIN is the required identification number for a customer that is a U.S. person and one of the possible identification numbers for a customer that is a non-U.S. person.

[6] The terms account and customer are defined at 31 C.F.R. § 1020.100(a) and (b), respectively.

banks (and their subsidiaries[7]) subject to the Board's jurisdiction, to instead use an alternative collection method to obtain TIN information from a third-party source rather than the customer, provided that the bank otherwise complies with the CIP Rule, which requires written procedures that: (1) enable the bank to obtain TIN information prior to opening an account; (2) are based on the bank's assessment of the relevant risks; and (3) are risk-based for the purpose of verifying the identity of each customer to the extent reasonable and practicable, enabling the bank to form a reasonable belief that it knows the true identity of each customer. The use of this exemption by banks is optional; banks are not required to use an alternative collection method for TIN information.

Background

FinCEN and the Agencies recognize that considerable changes in the way that customers interact with banks and receive financial services have occurred since 2001, when section 326 of the USA PATRIOT Act was enacted into law. The importance of collecting TIN information from the customer rather than through another method for identification and verification purposes has lessened since regulations implementing section 326 were adopted in 2003, particularly in light of the availability of new methods that a bank can use alongside TIN information to form a reasonable belief that the bank knows the true identity of each customer. As a result, in March 2024, FinCEN, in consultation with staff at the Agencies, issued a CIP Request for Information (the "CIP RFI") that sought information from the public to understand the potential risks and benefits, as well as safeguards that could be established, if banks were permitted to obtain part or all of a customer's TIN information from a third-party source prior to opening an account rather than from the customer.[8] FinCEN and the Agencies considered comments received through the CIP RFI, as well as the significant innovation in identity verification tools available to banks and other factors as described below, in granting this exemption from one aspect of the CIP TIN collection requirements.

Regulatory Requirements

The legislative framework generally referred to as the Bank Secrecy Act (BSA), which consists of the Currency and Foreign Transactions Reporting Act of 1970, as amended by the USA PATRIOT Act and other legislation, including the Anti-Money Laundering Act of 2020, is designed to combat money laundering (ML), the financing of terrorism (TF), and other illicit finance activity.[9] One of the main purposes of the BSA enumerated by Congress is to prevent the laundering of money and the financing of terrorism by requiring financial institutions to

---

[7] *See, e.g.,* 12 C.F.R. §§ 5.34(e)(3) and 5.38(e)(3) (requirements governing operating subsidiaries of national banks and Federal savings associations); *see also* Agencies, FinCEN, Office of Thrift Supervision, and Department of the Treasury, *Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act* (Apr. 28, 2005), available at https://www.fincen.gov/resources/statutes-regulations/guidance/interagency-interpretive-guidance-customer-identification.

[8] FinCEN, *Request for Information and Comment on Customer Identification Program Rule Taxpayer Identification Number Collection Requirement*, 89 FR 22231 (Mar. 29, 2024).

[9] USA PATRIOT Act, Public Law 107-56, 115 Stat. 272 (2001). The AML Act was enacted as Division F, sections 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116-283, 134 Stat. 3388.

establish reasonably designed, risk-based programs to combat such risks.[10] To fulfill the purposes of the BSA, Congress has authorized the Secretary of the Treasury (Secretary) to administer the BSA, and the Secretary has delegated the authority to implement, administer, and enforce compliance with the BSA and its implementing regulations to the Director of FinCEN.[11]

Section 326 of the USA PATRIOT Act 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." 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."[12] In prescribing these regulations, the Secretary must "take into consideration the various types of accounts maintained by various types of financial institutions, the various methods of opening accounts, and the various types of identifying information available."[13] The USA PATRIOT Act requires that CIP regulations involving financial institutions under the jurisdictions of the Agencies shall be jointly issued with each Agency appropriate for such financial institution.[14]

In 2003, FinCEN and the Agencies jointly issued regulations implementing section 326 of the USA PATRIOT Act for banks, *i.e.*, the CIP Rule.[15] The CIP Rule sets minimum standards for customer identification and verification, as directed by the USA PATRIOT Act, by requiring each bank to implement written CIP procedures that enable the bank to form a reasonable belief that it knows the true identity of each customer, which include verifying the identity of the customer to the extent reasonable and practicable. The procedures must specify the customer identifying information that a bank will obtain from each customer prior to opening an account, including, at a minimum, the customer's name, date of birth (for an individual), address, and identification number, which is a TIN for U.S. persons.[16] Generally, to fulfill the CIP Rule's identification

---

[10] 31 U.S.C. § 5311(2).

[11] Treasury Order 180-01 (Jan. 14, 2020); *see also* 31 U.S.C. § 310(b)(2)(I) (providing that the FinCEN Director "[a]dminister the requirements of subchapter II of chapter 53 of this title, chapter 2 of title I of Public Law 91-508, and section 21 of the Federal Deposit Insurance Act, to the extent delegated such authority by the Secretary").

[12] 31 U.S.C. § 5318(l)(2).

[13] 31 U.S.C. § 5318(l)(3).

[14] *See* 31 U.S.C. § 5318(l)(4).

[15] *See, e.g.,* Agencies, FinCEN, and Office of Thrift Supervision, *Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks,* 68 FR 25090, 25103 (May 9, 2003) (codified at 31 C.F.R. § 1020.220). 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 C.F.R. § 1010 and 31 C.F.R. § 1020).

[16] 31 C.F.R. § 1020.220(a)(2)(i). For non-U.S. person customers, the required identification number may include, in addition to a TIN, a 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. 31 C.F.R. § 1020.220(a)(2)(i)(B). A bank's CIP may include procedures for opening an account for a customer that has applied for but has not received a TIN. In this case, the CIP must include

number requirement, a bank must obtain TIN information from the customer, except with respect to credit card accounts.[17]

The CIP Rule also requires that a bank's CIP contain procedures to verify customer identity through documentary methods, non-documentary methods, or a combination of both, within a reasonable time after the account is opened. Verification methods include checking government-issued identification documents (documentary means) or the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement (non-documentary means).[18]

The BSA provides the Secretary and the appropriate Agency with the authority to, by regulation or order, exempt any financial institution or type of account from the requirements of any regulation prescribed under section 326 of the USA PATRIOT Act.[19] Under implementing regulation 31 C.F.R. § 1020.220(b), the appropriate Agency, with the concurrence of FinCEN, may by order or regulation exempt any bank or type of account from the requirements of the CIP Rule. The CIP Rule requires FinCEN and the Agencies to consider whether the exemption is consistent with the purposes of the BSA and with safe and sound banking and permits consideration of other appropriate factors.[20]

Findings Supporting an Exemption

Since the CIP Rule was issued in 2003, FinCEN and the Agencies have observed a significant expansion in ways that consumers access financial services, along with a rise in reported customer reluctance to provide their full TIN due, in part, to data breaches and identity theft concerns. In recent years, FinCEN and the Agencies have received continued public interest through letters and comments from banks, trade associations, and Members of Congress in permitting alternative collection methods for products and services beyond credit card accounts.[21] In the CIP RFI, FinCEN acknowledged there are, and will be, other available customer identifying attributes that banks may obtain, some of which vary in accuracy and authenticity, that could be used holistically as part of a bank's risk-based verification procedures under the CIP Rule.

The comments submitted in response to the CIP RFI provide insight into the benefits of third-party source TIN collection as well as potential risks. FinCEN received comments from a variety of stakeholders—banks and bank trade associations, financial technology companies, community organizations, third-party organizations, and individuals. Those in support of

---

procedures to confirm that the application was filed before the customer opens the account and to obtain the TIN within a reasonable period of time after the account is opened. This ORDER applies only to TIN information.

[17] Regarding credit card accounts, the CIP Rule allows banks to obtain customer identification information from a third-party source prior to extending credit to the customer. 31 C.F.R. § 1020.220(a)(2)(i)(C).

[18] 31 C.F.R. § 1020.220(a)(2)(ii).

[19] 31 U.S.C. § 5318(l)(5).

[20] 31 C.F.R. § 1020.220(b).

[21] *See, e.g.,* 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.

alternative collection methods commonly referenced the success of the credit card exception and innovation in customer verification methods. Those opposed, among other concerns, suggested that alternative collection methods would increase costs on financial institutions that do not already use third-party verification services. They stated that, in lieu of obtaining TIN information from the customer, these institutions would instead need to direct limited resources towards third-party identity verification services for TIN retrieval. Several commenters questioned the reliability of third-party sources, with one bank trade association cautioning that the intended purpose of these types of vendors was not true fraud prevention or customer verification.

In arriving at their findings, FinCEN and the Agencies considered letters and comments received; FinCEN's technical analysis of BSA information; FinCEN's consultation with law enforcement agencies; and the Agencies' examinations of current CIP programs and procedures (which may have included such processes for credit card accounts at banks with appropriate oversight, policies, procedures, and identity verification tools). Based on the analysis of this information, FinCEN has not identified heightened ML/TF or other illicit finance risk solely relating to the method of collection of TINs, and the Agencies consider an alternative collection method for TIN information consistent with safe and sound banking. FinCEN and the Board therefore find there is a valid basis for an exemption to allow banks the option to use an alternative collection method for TIN information.

Evidence from the Credit Card Exception Supports Expansion to Other Types of Accounts

For over 20 years, the CIP Rule has allowed banks to obtain the identifying information required by the CIP Rule from a third-party source when a customer is opening a credit card account. For these accounts, the bank may obtain the identifying information about a customer, including a TIN, from a third-party source prior to extending credit to the customer. FinCEN and the Agencies recognized at the 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.[22] Commenters raised concerns during the CIP Rule comment period that customers applying for credit card accounts were reluctant to give out their complete TIN, especially through non-face-to-face means, due to consumer privacy and security concerns.[23] In the CIP Rule, FinCEN and the Agencies further acknowledged that imposing a direct collection requirement on banks that offer credit card accounts would likely 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. FinCEN and the Agencies referenced the legislative history of section 326, which indicated 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

[22] Agencies, FinCEN, and Office of Thrift Supervision, *Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks*, 68 FR 25090, 25103 (May 9, 2003) (codified at 31 C.F.R. § 1020.220).
[23] *Id*. at 25098.

the regulations should not impose requirements that are burdensome, prohibitively expensive, or impractical.[24]

Therefore, FinCEN and the Agencies included an exception in the final CIP Rule for credit card accounts only that allowed a bank broader latitude to obtain some information from the customer opening a credit card account and the remaining information from a third-party source, such as a credit reporting agency, prior to extending credit to a customer. In the CIP Rule, FinCEN and the Agencies recognized this practice as an efficient and effective means of extending credit with little risk that the lender did not know the identity of the borrower.[25] Similar to credit card accounts, it is now common practice for banks to offer other types of products and services through non-face-to-face means, such as via a mobile app or website. For example, Forbes' 2022 Digital Banking Survey found that 78 percent of adults preferred banking over the internet rather than in person.[26] Additionally, customers are obtaining financial services using non-bank financial institutions at a significant rate. The FDIC's National Survey of Unbanked and Underbanked Households found that in 2023, half of all households (49.7 percent) were using non-bank online payment services, up from 46.4 percent in 2021.[27]

In light of these changes that have led to an increase in account openings using non-face-to-face means, FinCEN and the Board believe that the rationale relating to consumer privacy and security concerns provided for the credit card exception in 2003 as well as concerns about requirements being burdensome, prohibitively expensive, or impractical is applicable to all other types of accounts that are now easily accessible to customers through non-face-to-face means. Since the adoption of the credit card exception as part of the CIP Rule, FinCEN has not identified heightened ML/TF or other illicit finance risks associated specifically with the alternative collection method used by banks when opening credit card accounts where such methods are appropriately managed.

Consumer Privacy and Security Concerns Regarding TIN Collection

The letters and comments received by FinCEN and the Agencies assert that there is an elevated risk of identity theft and data breaches occurring when the full TIN is obtained from the customer through non-face-to-face means. In addition, BSA filings indicate that perpetrators of fraud, including check fraud, often opened their accounts online with fraudulent or stolen identification information,[28] which could argue for the need for banks to have more rigorous, rather than less, information collection from the customer when accounts are opened through non-face-to-face means in order for banks to form a reasonable belief that they know the true

[24] House Committee on Financial Services, *Report on the Financial Anti-Terrorism Act of 2001*, H.R. Rep. No. 107-250, pt. 1, at 63 (2001).
[25] 68 FR at 25097.
[26] Forbes Advisor, *Consumer Banking Trends and Statistics* (Jan. 21, 2024), available at https://www.forbes.com/advisor/banking/banking-trends-and-statistics/.
[27] FDIC, National Survey of Unbanked and Underbanked Households (2023), available at https://www.fdic.gov/household-survey/2023-fdic-national-survey-unbanked-and-underbanked-households-report.
[28] FinCEN, *Financial Trend Analysis, Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023* (Sept. 2024), available at https://www.fincen.gov/sites/default/files/shared/FTA-Check-Fraud-FINAL508.pdf.

identity of the person opening the account. However, FinCEN's analysis of BSA filings does not suggest that the risk of fraud was related to the method for obtaining customer information by a bank, whether from the customer or from a third party. Additionally, the American Bankers Association Banking Journal reported in 2023 that the SSN was the second most exposed individual credential after name.[29] During the first quarter of 2024, TransUnion reported that data breach risks rose significantly due to the high level of SSN exposures.[30] These statistics underscore the consumer hesitancy to provide the consumer's TIN through non-face-to-face means, and through this exemption, FinCEN and the Board will allow banks the means to obtain the customer's TIN through alternative collection methods.

Reliable Alternatives Exist for Verification Today that Did Not Exist or Were Not as Prevalent Twenty Years Ago

Reliable alternative processes for verification—which allow the bank to form a reasonable belief that it knows the true identity of each customer—are more prevalent today than when the CIP Rule was issued, meaning there could be circumstances in which such processes produce an equivalent or more reliable outcome when banks are permitted the flexibility to change their method of TIN collection based on the bank's assessment of the relevant risks. The combination of the increase in vulnerability of TINs to identity theft and the availability of reliable alternative options for verification lessens the importance of the specific method of TIN collection for identity verification.

While FinCEN and the Board are not prescribing specific alternative processes for banks, such processes should take into consideration the purpose of the CIP Rule—to ensure a bank is able to form a reasonable belief that it knows the true identity of each customer—and the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank's size, location, product and service offerings, and customer base.

Potential Risks of Alternative TIN Collection Methods

FinCEN received comments in response to the CIP RFI that raised concerns about increased risk when TIN information is not obtained from the customer. A commenter noted that the Internal Revenue Service (IRS) issued guidance in 2020 that it considers a SSN masked when only the last four digits are visible, which the commenter noted raises concerns that the last four SSN digits may be more readily compromised than the full TIN.[31] Similarly, one state bank association said their members stated it is easier for a fraudster to guess the last four digits of a

[29] American Bankers Association Banking Journal, *Report: Synthetic identity fraud on rise* (Aug. 24, 2023), available at https://bankingjournal.aba.com/2023/08/report-synthetic-identity-fraud-on-rise/.
[30] *See*, *e.g.*, CUToday, *Severity of Data Breach Risks Hit Highest Level in Two Years During Q1, TransUnion Reports* (May 28, 2024), available at https://www.cutoday.info/Fresh-Today/Severity-of-Data-Breach-Risks-Hit-Highest-Level-in-Two-Years-During-Q1-TransUnion-Reports.
[31] IRS, *What are we doing to protect taxpayer privacy?* (Feb. 7, 2025), available at https://www.irs.gov/privacy-disclosure/what-are-we-doing-to-protect-taxpayer-privacy#:~:text=A%20masked%20SSN%20is%20an,*%2D**%2D1234.

consumer's SSN than provide all nine digits accurately. A bank trade association raised that the SSN continued to be a strong customer identifier in comparison to the other identifying pieces of information a customer can provide. Individuals may undergo changes to their address, email, or phone number, but they rarely change their SSN.

With regard to potential increased fraud risk through alternative collection methods, FinCEN and the Board believe this is addressed because a bank's use of an alternative collection method must otherwise comply with the CIP Rule, which requires written procedures that: (1) enable the bank to obtain TIN information prior to opening an account; (2) are based on the bank's assessment of the relevant risks; and (3) are risk-based for the purpose of verifying the identity of each customer to the extent reasonable and practicable, enabling the bank to form a reasonable belief that it knows the true identity of each customer Further, these procedures (including use of an alternative collection method) must be based on the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank's size, location, and customer base.

Several commenters raised concerns that community banks and credit unions may not have the resources to implement the third-party TIN retrieval and verification service needed for an alternative TIN collection method and that implementing such a service could increase operational costs associated with account opening, which could negatively impact the unbanked. Therefore, smaller banks would be at a competitive disadvantage compared to larger banks. FinCEN and the Board emphasize there is no requirement to use this exemptive relief, and if a bank chooses to continue obtaining the full TIN from the customer, they may do so.

Some commenters raised issues that could occur if a bank only had the last four digits of a TIN. For example, some commenters stated that many people have the same last four digits. One stated that out of 119 people, there is a 50 percent chance that two will have the same last four; of 180 people, there is an 80 percent chance; and out of 300 people, there is more than 99 percent chance. The commenters stated this commonality could give rise to possible unintended consequences. For example, one commenter said it would be more complicated to create a "blacklist" for previously identified bad actors or place limitations on the number of accounts if only the last four digits are used. In addition, one entity stated this could increase concern for customers with common names or those using the same name (*e.g.*, Jr., Sr., III). FinCEN and the Board reiterate that if an alternative collection method is used, the bank must still obtain the full TIN from a third-party source prior to opening an account, and the TIN is one piece of customer identifying information among others that the bank must obtain and use to verify the customer's identity.

CONCLUSION

For the reasons described below, FinCEN and the Board find there is a valid basis for an exemption from the requirement to obtain TIN information from the customer for all accounts at all banks subject to the jurisdiction of the Board in the circumstances discussed herein. If banks use an alternative collection method when obtaining TIN information about a customer, they

must otherwise comply with the CIP Rule, which requires written procedures that: (1) enable the bank to obtain TIN information prior to opening an account; (2) are based on the bank's assessment of the relevant risks; and (3) are risk-based for the purpose of verifying the identity of each customer to the extent reasonable and practicable, enabling the bank to form a reasonable belief that it knows the true identity of each customer.

First, FinCEN finds this exemption, when used appropriately, is consistent with the purposes of the BSA. Banks must include an alternative collection method for TIN information in their existing, reasonably designed, risk-based, and written CIP procedures that combat ML/TF and other illicit finance activity. This exemption is also consistent with the factors discussed in the statute, including "the various types of accounts maintained by various types of financial institutions, the various methods of opening accounts, and the various types of identifying information available."[32] Furthermore, through an analysis of BSA reporting, FinCEN has not identified a heightened ML/TF or other illicit finance risk associated with the alternative collection method for TIN information process used by banks when opening credit card accounts.

Second, the Board finds this exemption, when used appropriately, would be consistent with safe and sound banking. The resulting banking practices will not be contrary to generally accepted standards of prudent banking operation and will not give rise to abnormal risk of loss or damage to an institution or its shareholders. This exemption does not change the overall purpose of the existing general CIP requirement for each bank to have CIP procedures that enable the bank to form a reasonable belief that it knows the true identity of each customer.

Therefore, FinCEN and the Board hereby grant by ORDER an exemption from a requirement of the CIP Rule implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l) in the circumstances discussed herein. Specifically, this Order provides an exemption from the CIP Rule that permits a bank to use an alternative collection method to obtain TIN information from a third-party rather than from the customer, provided that the bank otherwise complies with the CIP Rule, which requires written procedures that: (1) enable the bank to obtain TIN information prior to opening an account; (2) are based on the bank's assessment of the relevant risks; and (3) are risk-based for the purpose of verifying the identity of each customer to the extent reasonable and practicable, enabling the bank to form a reasonable belief that it knows the true identity of each customer.

Nothing in this ORDER shall bar, estop, or otherwise prevent the Board from taking any action affecting a bank, including the revocation of this ORDER, if a bank uses an alternative method for TIN collection but is not able to demonstrate its ability to form a reasonable belief that it knows the true identity of each customer.

Banks taking advantage of this exemption must continue to comply with all other regulatory requirements pursuant to the BSA.

[32] 31 U.S.C. § 5318(l)(3). These factors are mentioned in the statute in the context of what the Secretary should take into consideration when prescribing regulations.

IT IS SO ORDERED, this 31st day of July, 2025

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

By: _____/s/_____

Benjamin W. McDonough
Deputy Secretary of the Board

WITH CONCURRENCE, this 31st day of July, 2025
OF THE FINANCIAL CRIMES ENFORCEMENT NETWORK

By: _____/s/_____

Andrea M. Gacki
Director