

SUBJECT: BSA: Customer Identification Program and Customer Due Diligence

INTRODUCTION	1	Identifying Beneficial Owners	17
EXECUTIVE SUMMARY	1	Verifying Identities of Beneficial Owners	19
Customer Identification Program	2	Exemptions	19
Customer Due Diligence	2	Recordkeeping	19
Other ii Releases	3	IOLTA Accounts	20
CUSTOMER IDENTIFICATION PROGRAM	3	Accounts Opened Before May 11, 2018	20
Program Elements	3	FinCEN's Exemptive Relief from Beneficial Ownership Requirements for Legal Entity Customers of Rollovers, Renewals, Modifications, and Extensions of Certain Accounts	20
Developing CIP Procedures	3	Beneficial Owners & OFAC	21
Definitions	4	Beneficial Owners & 314(a) Requests	21
Customer Information Required	4	EXHIBIT A – PROCEDURE FOR GATHERING IDENTITY INFORMATION AT ACCOUNT OPENING – INDIVIDUALS (U.S. Citizen by Birth or Naturalization)	22
Customer Verification	5	EXHIBIT B – PROCEDURE FOR GATHERING IDENTITY INFORMATION AT ACCOUNT OPENING – INDIVIDUALS (Not a U.S. Citizen)	23
Recordkeeping and Retention	7	EXHIBIT C – PROCEDURE FOR GATHERING IDENTITY INFORMATION AT ACCOUNT OPENING – ORGANIZATION (Established or/Organized Under U.S. Law)	24
Comparison with Government Lists	7	EXHIBIT D – PROCEDURE FOR NON-DOCUMENTARY VERIFICATION	25
Member/Customer Notice	8	EXHIBIT E – CIP GUIDE	26
Reliance on other Financial Institutions	8	EXHIBIT F – FREQUENTLY ASKED QUESTIONS ABOUT CIP	27
CIP & Prepaid Cards	8	EXHIBIT G – CDD RISK MATRIX FOR INDIVIDUALS	36
CDD: RISK PROFILES, MONITORING & ENHANCED DUE DILIGENCE	10	EXHIBIT H – CDD RISK MATRIX FOR ORGANIZATIONS	38
Background	10	EXHIBIT I – FINCEN'S FREQUENTLY ASKED QUESTIONS REGARDING CDD (MAY 2026)	40
Establishing Risk-Based CDD Procedures	10		
Gathering Information & Developing Member/Customer Risk Profiles	11		
Conducting Ongoing Monitoring	12		
Using Enhanced Due Diligence for Higher-Risk Members/Customers	12		
Due diligence & money services businesses (MSBs)	14		
CDD: IDENTIFYING BENEFICIAL OWNERS OF LEGAL ENTITIES	15		
"Legal entity customer"	15		
"Beneficial Owners"	16		
"Account"	17		

INTRODUCTION

This release applies to all state and federal credit unions. It describes requirements for credit unions to verify the identities of those who open new accounts, to identify higher-risk members/customers, to monitor higher-risk members/customers and their accounts with enhanced due diligence, and to gather information about the beneficial owners of legal entity members.

EXECUTIVE SUMMARY

As part of their Bank Secrecy Act / Anti-Money Laundering (BSA/AML) compliance programs, credit unions and other covered financial institutions (such as banks) must adopt effective procedures that help them understand who their customers/members are and what types of transactions they conduct. This requirement is found in BSA/AML regulations issued by the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN).

Four core elements are fundamental to these procedures, FinCEN says:

1. Identifying and verifying the identity of customers/members;
2. Identifying and verifying the identity of beneficial owners of legal entity customers/members (i.e., the natural persons who own or control legal entities);
3. Understanding the nature and purpose of customer relationships to develop a member/customer risk profile; and

4. Conducting ongoing monitoring for reporting suspicious transactions and, on a risk adjusted basis, maintaining and updating member/customer information.

The first element is covered by FinCEN's "Customer Identification Program" (CIP) rules. The remaining three elements are covered by FinCEN's "Customer Due Diligence" (CDD) rules.

This release summarizes both the CIP and CDD requirements.

Customer Identification Program

All U.S. financial institutions must establish minimum procedures for identifying and verifying the identity of members/customers who open new accounts.

Every credit union must have a written Customer Identification Program (CIP) that is appropriate for its size, location and type of business. At a minimum, it must address each of the following:

- *Customer information required.* The identifying information that will be obtained at account opening.
- *Customer verification.* The procedures for verifying the identity of the member/customer using the member/customer information obtained. Describe when the credit union will use documents, non-documentary methods, or a combination of methods.
- *Recordkeeping and retention.* The procedures for maintaining records that include the member/customer information obtained for five years after the account is closed; and a description of the method(s) used to verify identity and a description of the resolution of any substantive discrepancy for five years after the record is made.
- *Comparison with government lists.* The procedures for determining whether the member/customer appears on any list of known or suspected terrorists issued by the U.S. Treasury.
- *Customer notice.* The procedures for notifying members/customers that the credit union is requesting information to verify their identities.
- *Reliance on other financial institutions.* Optional procedures specifying when the credit union may rely on another financial institution to perform any part of the credit union's CIP.

The League offers a Customer Identification Card (WCUL #81080) to help credit unions comply with CIP requirements.

In addition to deterring money laundering and terrorist financing, CIP helps protect consumers against fraud, including identity theft.

Customer Due Diligence

FinCEN's BSA regulations require credit unions and other covered institutions (including banks) to have written, risk-based procedures for conducting CDD as part of their BSA/AML compliance programs.

There are two aspects to the FinCEN's CDD requirements:

- One aspect of the CDD rules requires risk-based procedures for conducting ongoing CDD to understand the nature and purpose of member/customer relationships so that the credit union can develop a member/customer risk profile and monitor for suspicious activity. To comply, a credit union's CDD procedures should basically cover three steps:
 1. Gathering information to develop a "customer risk profile" at account opening.
 2. Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintaining and updating "customer information."
 3. Applying enhanced due diligence to higher-risk customers/members.
- Another aspect of the CDD rules requires credit unions to have written procedures to identify "beneficial owners" – the people who own and control "legal entity customers" – organizations opening credit union accounts. Credit unions then must verify the identities of those beneficial owners. Additionally, credit unions must establish procedures for making and maintaining a record of all of the identification and verification information collected.

Due diligence & money services businesses

Regulators have special BSA/AML compliance expectations for credit unions serving money services businesses. That's a term used by financial regulators to describe a business that isn't a bank or credit union but that provides some bank-like services, including currency dealers or exchangers, check cashers, issuers or sellers of traveler's checks or money orders, money transmitters, and providers or sellers of prepaid access. If your credit union serves MSBs, then the NCUA expects it to consider, monitor, and mitigate the risks by developing policies, procedures, and processes to achieve certain goals.

Other ii Releases

Several other ii Releases address different aspects of BSA compliance:

- *ii Release No. 0071 – Bank Secrecy Act.*
- *ii Release No. 0109 – BSA: Suspicious Activity Reports.*
- *ii Release No. 0187 – BSA: Money Services Businesses*

CUSTOMER IDENTIFICATION PROGRAM

Federal regulations require each credit union to implement a CIP policy approved by its board of directors. The CIP policy must be written, and it must be part of the credit union's BSA/AML policy/program; it is not a separate program.

The credit union's board of directors is responsible for approving a Customer Identification Program in enough detail for the board to determine that it meets minimum regulatory requirements and is designed to enable the credit union to form a reasonable belief it knows the true identities of members/customers.

For more information on BSA/AML program requirements, see *ii Release No. 0071, "Bank Secrecy Act."*

Program Elements

All U.S. financial institutions must establish minimum procedures for identifying and verifying the identity of members/customers who open new accounts.

Every credit union must have a written Customer Identification Program that is appropriate for its size, location and type of business. At a minimum, it must address each of the following:

- *Customer information required.* The identifying information that will be obtained at account opening.
- *Customer verification.* The procedures for verifying the identity of the member/customer using the member/customer information obtained. Describe when the credit union will use documents, non-documentary methods, or a combination of methods.
- *Recordkeeping and retention.* The procedures for maintaining records that include the member/customer information obtained for five years after the account is closed; and a description of the method(s) used to verify identity and a description of the resolution of any substantive discrepancy for five years after the record is made.
- *Comparison with government lists.* The procedures for determining whether the member/customer appears on any list of known or suspected terrorists issued by the U.S. Treasury.
- *Customer notice.* The procedures for notifying members/customers that the credit union is requesting information to verify their identities.
- *Reliance on other financial institutions.* Optional procedures specifying when the credit union may rely on another financial institution to perform any part of the credit union's CIP.

The League offers a Customer Identification Card (WCUL #81080) to help credit unions comply with CIP requirements.

Developing CIP Procedures (31 C.F.R. § 1020.220)

Credit union management must develop risk-based CIP procedures for verifying the identity of each member/customer to the extent reasonable and practicable, using identifying documents that identify the member/customer and/or using non-documentary verification methods such as checking information against third-party databases.

No sample procedures are included in this release since credit unions must tailor procedures to their own circumstances, consistent with the CIP policy that the board approves as part of the credit union's BSA/AML policy. The release does include several exhibits designed to help show steps a credit union might consider as it drafts its own procedures.

Definitions

The CIP rules apply to "Accounts" of all "Customers" defined as:

- *Account.* A formal banking relationship established to provide or engage in services, dealings, or other financial transactions including deposit accounts, transaction or asset accounts, loans and other forms of credit, safe deposit box rentals, safekeeping services, cash management, and custodian and trust services.

"Account" does not include:

- Check cashing, wire transfers, or the sale of checks or money orders, if no formal banking relationship is established;
- An account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974; or
- Accounts the credit union acquires through an acquisition, merger, purchase of assets, or assumption of liabilities from any third party, unless it would be appropriate for the credit union, as part of due diligence procedures required under existing BSA regulations, to verify the identity of customers associated with acquired accounts.
- *Customer.* An individual or legal entity that is opening a new Account with the credit union. Customer also means an individual who is opening a new Account for another individual who lacks legal capacity (such as a minor or an incompetent person) or for a group that has not formed a legal entity (such as a sunshine club or bowling league). In the case of joint Accounts, it means each accountholder.

"Customer" does not include:

- A person with an existing Account, provided that the credit union has a reasonable belief that it knows the true identity of the Customer; or
- Financial institutions regulated by federal functional or state bank regulators, governmental agencies and instrumentalities, and companies that are publicly traded (domestic operations).
- *Authorized Signers.* While the definition of "Customer" in the CIP rules does not include a signatory for an organization account (e.g., a trust or a corporation), you may want to obtain information about individuals with authority or control over an account, including signatories. The CIP rules say that your policy should address when you will opt to conduct CIP for authorized signers on an organization account. See the section labeled "Additional Verification for Certain Members/Customers."

Customer Information Required

The CIP procedures must specify the identifying information a credit union will obtain from a member/customer. At a minimum, a credit union must obtain from each member/customer the following information *before* opening an account:

- Name.
- For individuals, date of birth.
- An address, which must be:
 - For individuals, a residential or business street address.
 - For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual.
 - For an individual in a state's "address confidentiality program," use the street address of the program's sponsoring agency as "another contact individual." These programs are designed to protect victims of domestic abuse. Participants are given a post office box address where mail is received on their behalf. The agency forwards the mail to the participant's actual address.
 - For persons other than individuals, such as corporations and trusts, the address of the principal place of business, local office or other physical location.

- An identification number, which must be:
 - For U.S. persons (i.e., an individual who is a U.S. citizen, or an entity established or organized under the laws of a State or the United States), a U.S. taxpayer identification number (Social Security number, individual taxpayer identification number or employer identification number).
 - For non-U.S. persons (i.e., an individual that does not meet the criteria of a U.S. Person), one or more of the following: a U.S. taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard (e.g., biometric identifiers may be used in addition to or instead of photographs).

Based on its risk assessment, a credit union may require additional identifying information for certain members/customers or product lines.

TIN Applied For

The rule affords some flexibility when a member/customer has applied for but not yet received a TIN. Instead of obtaining a TIN from a member/customer prior to opening an account, the CIP procedures can allow the credit union to confirm that the TIN application was filed before the member/customer opens the account and to obtain the TIN within a reasonable time after the account is opened. The credit union can exercise its discretion to determine how to confirm that a member/customer has filed an application for a TIN rather than having to keep a copy of the application on file. For example, a credit union may wish to examine a copy of the application filed.

Credit Card Accounts

There is an exception for credit card accounts that permits credit unions offering such accounts to acquire information about the member/customer, including the identification number, from a trusted third party source prior to extending credit to the member/customer, rather than having to obtain this information directly from the member/customer before opening the account.

Customer Verification

A credit union must have procedures for verifying the identity of the member/customer “using identifying information obtained by the institution.” Therefore, a credit union does not need to establish the accuracy of every element of identifying information it obtains, but it must do so for enough information to form a reasonable belief that it knows the true identity of the member/customer. The credit union must verify the member’s/customer’s identity within a reasonable time after the account is opened.

The CIP procedures must describe when it will use documents, non-documentary methods or a combination of both methods to verify a member’s/customer’s identity.

Verification through Documents

The CIP procedures must describe when the credit union will verify identity through documents and list the documents that it will use.

These documents may include (among others):

- *For individuals.* Unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver’s license or passport;
 - *For elderly or disabled individuals.* The U.S. Treasury’s Administrative Ruling 92-1 provides guidance on how a credit union can verify the identity of an elderly or disabled member/customer who does not have the normally acceptable forms of identification. A credit union may accept a Social Security, Medicare, or Medicaid card along with another form of documentation bearing their name and address. Additional forms of documentation include a utility bill, a tax bill, or a voter registration card. The forms of alternate identification a credit union decides to accept should be included in its policies, procedures, and processes.
- *For corporations, partnerships, trusts and persons other than individuals.* Documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, partnership agreement, or trust instrument.

A credit union may generally rely on government-issued identification as verification of a member’s/customer’s identity. A credit union is not required to determine whether the document has been validly issued; however, if a document shows obvious signs of

fraud, the credit union must consider that fact in determining whether it can form a reasonable belief that it knows the member's/customer's true identity.

Credit unions are encouraged to obtain more than one type of documentary verification to ensure they have a reasonable belief about a member's/customer's true identity. They should also use a variety of methods to verify the identity of a member/customer, especially when they cannot examine original documents.

Non-documentary Verification Methods

The CIP procedures must describe the non-documentary methods the credit union will use to verify a member's/customer's identity and when these methods will be used in addition to, or instead of, relying on documents.

Non-documentary methods may include: contacting a member/customer; independently verifying the member's/customer's identity by comparing information provided by the member/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.

- For organizations, you may want to check Wisconsin DFI's Corporate Records Search at <https://apps.dfi.wi.gov/apps/corpsearch/search.aspx>

The credit union's non-documentary procedures must address situations where:

- An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
- The credit union is not familiar with the documents presented;
- The account is opened without obtaining documents;
- The member/customer opens the account without appearing in person at the credit union (this includes accounts opened via the telephone, mail, or the Internet); or
- Circumstances that increase the risk that the credit union will be unable to verify the true identity of a member/customer through documents.

Because identification documents may be obtained illegally and may be fraudulent and in light of the recent increase in identity theft, credit unions are encouraged to use non-documentary methods even when the member/customer has provided identification documents.

Additional Verification for Certain Members/Customers

The CIP procedures must address situations where, based on the credit union's risk assessment of a new account opened by a non-individual (e.g., a trust or a corporation), the credit union will obtain information about individuals with authority or control over the account, including authorized signers, to verify the member's/customer's identity. However, the credit union may want to do CIP on authorized signers in every case. According to America's Credit Unions, "It would be a good best practice for the credit union to collect information from business account signatories since they have access to the funds in the account. ... In most cases, it has become customary for a financial institution to obtain information ... about individuals with control or authority over the business account (even signatories)."

A credit union does not need to undertake any additional verification if it chooses not to open an account when it cannot verify the member's/customer's identity using standard documentary and non-documentary verification methods.

Lack of verification

The CIP procedures must address what the credit union will do if it cannot form a reasonable belief that it knows the true identity of a member/customer. The procedures should describe the following:

- When the credit union should not open an account for a potential member/customer;
- The terms under which a member/customer may use an account while the credit union tries to verify the member's/customer's identity;
- When the credit union should close an account after trying to verify a member's/customer's identity have failed; and
- When the institution should file a Suspicious Activity Report (SAR). See The League's *ii Release No. 0109* for details on SARs.

The rule does not require a credit union to close an account of an individual whose identity cannot be verified, but instead leaves this to the credit union's discretion.

Keep in mind that a credit union must comply with other applicable laws and regulations, such as the Equal Credit Opportunity Act (ECOA) and the Fair Credit Reporting Act (FCRA), when determining not to open an account because it cannot establish a reasonable belief that it knows the true identity of the member/customer. Those regulations may require that an adverse action notice be sent. For more information, see *ii Release No. B041, "Reg. B – Equal Credit Opportunity,"* and *No. 0126, "Fair Credit Reporting Act."*

Recordkeeping and Retention

Your credit union's CIP procedures must provide for making and maintaining records of all CIP information you obtain. The regulations provide for a two-part record retention schedule.

- A credit union must retain the identifying information obtained about a member/customer for five years after the date the account is closed (or in the case of credit card accounts, five years after the account is closed or becomes dormant).
 - Name.
 - Address.
 - Date of birth for an individual.
 - Identification number.
 - Any other information required by the credit union's CIP.
- A credit union need only retain the other records it makes regarding the information that verifies a member's/customer's identity for five years after the record is made. The records must:
 - Describe any document which the credit union relied on to verify the identity of the member/customer. The description must note:
 - Identification number contained in the document;
 - Place of issuance; and,
 - Date of issuance and expiration date (if any).
 - Describe the methods and results of any steps taken to verify the identity of the member/customer; and
 - Describe the resolution of any substantive discrepancy discovered when verifying the identifying information.

You may use electronic records to satisfy the requirements of CIP regulations, as long as the records are accurate and remain accessible in accordance with the BSA regulations which say: "All such records shall be filed or stored in such a way as to be accessible within a reasonable period of time, taking into consideration the nature of the record, and the amount of time expired since the record was made." (12 C.F.R. § 1010.430(d)).

Keep in mind that the collection and retention of information about a member/customer, such as an individual's race or sex, as a part of collecting identifying information, do not relieve a credit union from its obligations to comply with anti-discrimination laws or regulations, such as the prohibition in the Equal Credit Opportunity Act against discrimination in any credit transaction on the basis of race, color, religion, national origin, sex, marital status, age, or other prohibited classifications. For more information, see The League's *ii Release No. B041, "Reg. B – Equal Credit Opportunity."*

Comparison with Government Lists

The CIP procedures must provide for determining whether the member/customer appears on any list of known or suspected terrorists or terrorist organizations provided to the credit union by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. Your CIP procedures must require the credit union to make such determination within a reasonable time after the account is opened, or earlier, if required by another federal law or regulation or federal directive issued in connection with the applicable list. Your CIP procedures must also ensure that the credit union follows all federal directives issued in connection with such lists.

Treasury and the federal regulators (including NCUA) have not yet designated any such lists; therefore, the CIP regulations cannot be more specific about the lists credit unions must check.

Different rules bar credit unions and other financial institutions from handling transactions that involve any person or group that appears on various lists issued by the Office of Foreign Assets Control (OFAC). Specifically, credit unions and other financial institutions are required to block or "freeze" property and payment of any funds transfers or transactions involving those blocked countries or persons whose names appears on the OFAC lists, and to report the "blocks" within 10 days of occurrence. Failure to block and report an "illicit transfer" may subject the credit union to civil fines, and possibly criminal penalties. For more information, see The League's *ii Release No. 0148, "OFAC Compliance."*

Member/Customer Notice

Your CIP procedures must address how you will give credit union members/customers adequate notice that the credit union is requesting information to verify their identities. Notice is adequate if the credit union generally describes the identification requirements of the CIP regulations and gives notice in a way that is reasonably designed to ensure that a member/customer sees the notice or is otherwise given notice, before opening an account.

Depending on how an account is opened, your credit union may post a notice in the lobby or on its website, include the notice on its applications, or use any other form of oral or written notice.

The CIP regulations include the following sample notice language:

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

Reliance on other Financial Institutions

A credit union's CIP procedures may specify when it will rely on another financial institution (including an affiliate) to perform any part of the credit union's CIP. Reliance is permitted if a member/customer of the credit union is opening, or has opened, an account or has established a similar banking or business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions.

To rely on another institution, a three-part test must be met:

- Reliance must be reasonable under the circumstances;
- The other financial institution must be subject to the anti-money laundering compliance program requirements of the Bank Secrecy Act and be regulated by a federal functional regulator; and
- The other financial institution must enter into a contract requiring it to certify annually to the credit union that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) the specified requirements of the institution's CIP and that the institution has in fact agreed to perform those functions.

If the test is not met, then the credit union remains solely responsible for applying its own CIP to each member/customer. This provision can be considered a limited safe harbor.

Use of Third Parties

The CIP regulations do not affect a credit union's authority to contract for services to be performed by a third party, either on or off the credit union's premises. For example, a credit union may contract with a third party provider to keep its records even when the credit union does not act under the reliance provision. Because NCUA does not have specific statutory authority to regulate and examine service providers, the agency requires credit unions to document that their service providers fully comply with this regulation and with the credit union's CIP.

The CIP regulations do not alter a credit union's authority to use agents to perform services on its behalf. Therefore, a credit union is permitted to arrange for a car dealer or mortgage broker, acting as an agent in connection with a loan, to verify the identity of its member/customer. However, as with any other responsibility performed by an agent, the credit union is ultimately responsible for that agent's compliance with the requirements of the CIP regulations. There is no limited liability, as there would be if you relied on another financial institution, as explained above.

CIP & Prepaid Cards

The NCUA and other federal financial institution regulations issued *joint guidance* in 2015 to clarify how CIP requirements apply to issuers and users of prepaid cards.

This guidance clarifies that certain prepaid cards issued by a credit union should be subject to its CIP, including when a credit union issues prepaid cards under arrangements with third-party program managers that sell, distribute, promote, or market the prepaid cards issued by the credit union.

In order to determine if CIP requirements apply to purchasers of prepaid cards, the credit union should 1) determine whether the issuance of a prepaid card to a purchaser results in the creation of an “account” subject to CIP requirements; and if so, 2) identify the credit union’s member/customer to whom CIP applies.

Determining the existence of an “account”

According to the guidance, the following functions on a prepaid card means that an “account” has been created, triggering the need for CIP:

- Reloadable by the cardholder or another party on behalf of the cardholder;
- Withdrawals permitted in excess of the card balance; or
- Access to an overdraft line or an established line of credit.

Identifying the “customer”

Credit unions must understand who their customer/member is for CIP purposes. The answer varies, depending on the type of card and who is allowed to access it.

- *Payroll cards.* If the employer (or the employer’s agent) is the only person that may deposit funds into the payroll card account, the employer should be considered the credit union’s customer/member for CIP purposes. In that case, the credit union is not required to apply its CIP to each employee. The employer should be considered to be the customer/member even if there are subaccounts that are attributable to each employee. By contrast, if the employee may access credit through the card, or reload the payroll card account from sources other than the employer, the employee should be considered the customer/member and the credit union should apply its CIP to the employee.
- *Government benefit cards.* If a government benefits card program permits only government funds to be loaded onto the card and does not provide access to credit, no customer/member relationship is established between the credit union and the beneficiary-cardholder for purposes of the CIP rule. A credit union that issues such a government benefit card is not required to apply its CIP to the government agency establishing the benefit card account. If, however, the card allows non-government funds to be loaded onto the card or provides access to credit, then a customer/member relationship is established between the credit union and the beneficiary-cardholder and the credit union should collect CIP information from the beneficiary-cardholder.
- *Health benefit cards.* Health Savings Accounts (HSA), Flexible Spending Arrangements (FSA), and Health Reimbursement Arrangements (HRA) are all used to set aside tax-exempt funds for certain medical expenses. Because the employee establishes the HSA, the employee is the issuing credit union’s customer/member for purposes of the CIP rule. Because no person other than the employer (or employer’s agent) establishes an FSA or HRA, makes deposits into the FSA or HRA, and distributes funds from the FSA or HRA, the employer should be the issuing credit union’s customer/member for purposes of the CIP rule.
- *Closed-loop cards.* In the case of closed-loop prepaid cards, those that do not have the functionalities that trigger the CIP rule, such as a specific retailer’s card, the third-party program manager in whose name the pooled account has been established should be considered to be the only customer/member of the issuing credit union and subject to the CIP requirements. In these cases, the issuing credit union is not required to “look through” the pooled account to verify the identity of each cardholder.

Prepaid cards & third parties

In a footnote to the guidance, NCUA notes that any credit union contemplating entering into an account relationship involving holders of prepaid cards sold and distributed by third parties must ensure that the consumer with whom the credit union intends to establish the relationship is within the credit union’s field of membership.

Additionally, the guidance emphasizes that issuing credit unions should enter into well-constructed, enforceable contracts with third-party program managers that clearly define the expectations, duties, rights, and obligations of each party. At a minimum, the agreement should:

- Outline CIP obligations of the parties;
- Ensure the right of the issuing credit union to transfer, store, or otherwise obtain immediate access to all CIP information collected by the third-party program manager on cardholders; and

- Provide for the issuing credit union's right to audit the third-party program manager and to monitor its performance.

The guidance also points out that credit unions must comply with *Letter to Credit Unions 07-CU-13* and the accompanying *Supervisory Letter 07-01* – which set standards for NCUA examiners to review a credit union's third party relationships.

CDD: RISK PROFILES, MONITORING & ENHANCED DUE DILIGENCE

(31 C.F.R. §1020.210)

FinCEN's BSA regulations require credit unions and other covered institutions (including banks) to have written, risk-based CDD procedures as part of their BSA/AML compliance programs.

There are two aspects to the FinCEN's CDD requirements:

- One aspect of the CDD rules (covered in this section of the release) requires risk-based procedures for conducting ongoing CDD 1) to understand the nature and purpose of member/customer relationships to develop a member/customer risk profile; and 2) to conduct ongoing monitoring for suspicious transactions and, on a risk adjusted basis, maintain and update member/customer information.
- Another aspect of the CDD rules (covered in the next section of the release) requires credit unions to have written procedures to identify "beneficial owners" – the people who own and control "legal entity customers" – organizations opening credit union accounts. Credit unions then must verify the identities of those beneficial owners. Additionally, credit unions must establish procedures for making and maintaining a record of all of the identification and verification information collected.

Background

Prior to 2018, FinCEN did not explicitly require credit unions or other covered financial institutions to engage in CDD, though regulators and examiners expected it and said it was "implicitly required" by BSA suspicious activity reporting obligations. The Federal Financial Institutions Examination Council (FFIEC), a group of federal financial regulators including the NCUA, spelled out CDD expectations in its *Bank Secrecy Act/Anti-Money Laundering Examination Manual*:

The cornerstone of a strong Bank Secrecy Act/Anti-Money Laundering (BSA/AML) program is the adoption of comprehensive CDD policies, procedures and processes for all members/customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD should be to enable the credit union to predict with relative certainty the types of transactions in which a member/customer is likely to engage. These processes assist the credit union in determining when transactions are potentially suspicious. The concept of CDD begins with verifying the member's/customer's identity and assessing the risks associated with that member/customer. Processes should also include enhanced CDD for higher-risk members/customers and ongoing due diligence of the member/customer base.

In 2016, FinCEN amended its BSA regulations to explicitly require credit unions and other covered institutions (including banks) to have written, risk-based procedures for conducting ongoing CDD. Compliance with this requirement is mandatory as of May 11, 2018.

This release includes several CDD-related exhibits, including CDD risk matrices and a set of Frequently Asked Questions about CDD from FinCEN.

Establishing Risk-Based CDD Procedures

FinCEN's BSA regulations establish five "pillars" – the fundamental requirements for BSA compliance. The fifth pillar (§1020.210 (b)(5)) addresses CDD. It requires a credit union's BSA/AML program to include, at a minimum:

- (5) Appropriate risk-based procedures for conducting ongoing customer due diligence, to include, but not be limited to:
 - (i.) Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
 - (ii.) Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

The regulations do not go on to explicitly spell out what a credit union's CDD procedures must address. However, the FFIEC's *BSA/AML Examination Manual* provides useful guidance on CDD. It says that a credit union's BSA/AML policies, procedures and processes should:

- Fit the credit union's risk profile, paying particular attention to higher-risk members/customers.
- Contain a clear statement of management's expectations, including who is responsible for reviewing or approving changes to a member's/customer's risk profile.
- Ensure that the credit union has enough member/customer information to implement an effective suspicious activity monitoring system.
- Provide guidance for documenting analysis.
- Ensure that the credit union maintains current member/customer information.

To fulfill FFIEC's expectations, a credit union's CDD program should cover three key steps:

1. Gathering information to develop a member/customer risk profile at account opening.
2. Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintaining and updating member/customer information.
3. Applying enhanced due diligence to higher-risk members/customers.

The remainder of this section of the release will explore each of the three steps.

Gathering Information & Developing Member/Customer Risk Profiles

The CDD regulations require credit unions need to have risk-based procedures for conducting ongoing CDD "to include understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile."

According to FinCEN, the term "customer risk profile" refers to the information gathered about a member/customer at account opening. (FinCEN uses the term "customer" instead of member, and so we use the same term in this release.) The profile is used to develop a baseline against which member/customer activity is assessed for suspicious activity reporting. (BSA requires credit unions and other to report "suspicious activity," including transactions that are not of the sort the member would be normally expected to engage in. CDD helps credit unions know what kinds of account activity they should expect from members.)

According to the FFIEC *BSA/AML Examination Manual*, at account opening, the credit union should gather enough information about the member/customer to understand what level of normal activity to expect for the member's/customer's occupation or business operations. The examiners expect to see processes in place to obtain information at account opening as well as ensuring that "current" member/customer information is maintained.

Management should assess account risk on the basis of a variety of factors, which may include:

- The type of account and its size;
- The types and frequency of transactions;
- The country of residence of the principals or beneficiaries, or the country where established, or source of funds; and
- Accounts and transactions that are not usual and customary for the member or for the credit union.

FinCEN says that "the customer risk profile may include self-evident information such as the type of customer or type of account, service, or product."

According to the FFIEC *BSA/AML Examination Manual*, much of the CDD information can be confirmed through an information-reporting agency, banking references (for larger accounts), correspondence and telephone conversations with the member, and visits to the member's place of business. Additional steps may include obtaining third-party references or researching public information (e.g., on the Internet or commercial databases).

This release includes two tools to help credit union staff gather information and assess risks that new members/customers pose: Exhibit G – CDD risk matrix for individuals; and Exhibit H – CDD risk matrix for organizations. Note, however, that when FinCEN published its CDD regulations, it said: "The [Customer] profile may, but need not, include a system of risk ratings or categories of customers." Thus, credit unions may want to, but do not necessarily have to, assign risk ratings at account openings. Regardless, they should identify members that are high-risk and warrant enhanced due diligence, as explained later in this release.

Conducting Ongoing Monitoring

FinCEN says that an effective CDD program involves ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update “customer information.” (“Customer information” includes information about the beneficial owners of legal entities that open credit union accounts, as explained in the next section of this release.)

According to the FFIEC *BSA/AML Examination Manual*, the objective of CDD is for the credit union to predict “with relative certainty” the kinds of transactions a member is likely to conduct, in order to help spot suspicious transactions.

BSA requires credit unions and other to report “suspicious activity,” including transactions that are not of the sort the member would be normally expected to engage in. To do this, you will need to rely on the “customer profile” information you gather at account opening, which should help you to understand what level of normal activity to expect for the member’s occupation or business operations. For more information, see *ii Release No. 0109, “BSA: Suspicious Activity Reports.”*

The CDD risk matrices attached as Exhibits G and H can be used to help track changes in member/customer risk levels.

Updating CDD Information

When FinCEN published its CDD regulations, it explained when & how credit unions are to update their CDD risk profiles and member/customer information:

When a financial institution detects information (including a change in beneficial ownership information) about the customer in the course of its normal monitoring that is relevant to assessing or reevaluating the risk posed by the customer, it must update the customer information, including beneficial ownership information. Such information could include, e.g., a significant and unexplained change in the customer's activity, such as executing cross-border wire transfers for no apparent reason or a significant change in the volume of activity without explanation. It could also include information indicating a possible change in the customer's beneficial ownership, because such information could also be relevant to assessing the risk posed by the customer.

This provision does not impose a categorical requirement that financial institutions must update customer information, including beneficial ownership information, on a continuous or periodic basis. Rather, the updating requirement is event-driven, and occurs as a result of normal monitoring.

Using Enhanced Due Diligence for Higher-Risk Members/Customers

Your policies and procedures should provide for staff to identify, at account opening, members/customers that pose a heightened risk for money laundering, terrorist financing, or other illegal activity. If such members/customers are identified, then you must apply what the FFIEC calls “enhanced customer due diligence.”

Identifying Higher-Risk Members/Customers

Although any type of member/customer is potentially vulnerable to money laundering or terrorist financing, the FFIEC manual says that certain members/customers may pose higher money laundering risks because of their business, occupation, or anticipated transaction activity. These include:

- Non-bank financial institutions (e.g., money services businesses, casinos and card clubs, brokers/dealers in securities, and dealers in precious metals, stones or jewels);
- Nonresident aliens, foreign individuals and foreign entities;
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately-owned ATMs, vending machine operators, and parking garages);
- Non-governmental organizations and charities (foreign and domestic);
- Professional service providers (e.g., attorneys, accountants, doctors, and real estate brokers); and
- Deposit brokers.

The Manual describes other potentially high-risk persons and entities, but they are uncommon for Wisconsin credit unions. Contact The League for guidance on special due diligence rules if your credit union has correspondent accounts with foreign banks, private banking arrangements with non-U.S. persons, or relationships with foreign embassies, consulates or missions.

Exercise judgment and do not simply define or treat everyone in a specific category as posing the same level of risk. Consider other variables, such as the services that are being provided, sources of funds, and geographic locations.

For more information on these types of members/customers and the risks they pose, as well as an overview of compliance requirements and explanations of examination procedures, see the FFIEC *Bank Secrecy Act/Anti-Money Laundering Examination Manual*.

The CDD risk matrices attached as Exhibit G and H can be used to help track changes in member/customer risk levels.

Enhanced Due Diligence

If you identify members/customers that pose a higher-risk for money laundering, terrorist financing, or other illegal activity, you must apply enhanced due diligence. This requires increased scrutiny of the member/customer and their transactions at account opening and more frequently throughout the term of their relationship. For example, you will need to review aggregate cash activity, wire transfers, and CTR transactions more frequently.

If you determine that a member/customer poses a higher-risk because of the member's/customer's business activity, ownership structure, anticipated or actual volume and types of transactions, (including transactions in high-risk jurisdictions), then consider obtaining, both at account opening and throughout the relationship, the following information:

- Purpose of the accounts.
- Source of funds and wealth.
- Beneficial owners of the accounts, as applicable.
- Member's/customer's (or beneficial owner's) occupation or type of business.
- Financial statements.
- Banking references.
- Domicile (where the business is incorporated).
- Proximity of the member's/customer's residence, place of employment, or place of business to the credit union.
- Description of the business' primary trade area and whether international transactions are expected to be routine.
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers.
- Explanations for changes in account activity.

Unlawful Internet Gambling

The Federal Reserve's Reg. GG requires the credit union to conduct due diligence when opening commercial accounts to determine the risk that a member business may operate an Internet gambling business. For details The League's *ii Release No. 0177*.

Marijuana-related businesses

If the credit union serves marijuana-related businesses, see the special guidance from FinCEN in *FIN-2014-G001 BSA Expectations Regarding Marijuana-Related Businesses (February 14, 2014)*. A portion of that guidance is reprinted in *Exhibit A - Filing suspicious activity reports on marijuana-related businesses in ii Release No. 0109*. *FIN-2014-G001* also includes FinCEN's due diligence considerations and red flags for financial institutions serving marijuana-related businesses. The special guidance is necessary because production, sale, and possession of marijuana, even medical marijuana is a crime under federal law, regardless of whether it is legal under state law.

Make no mistake: marijuana is currently illegal under Wisconsin law - including medical marijuana.

Hemp and CBD can be legal - if the current requirements under state and federal law are met. If the credit union services hemp or CBD businesses, it is advisable to be prepared (policies, training, and procedures) to comply with FinCEN's marijuana-related business guidance. The credit union could encounter products that don't qualify as legal hemp or CBD, so are viewed as marijuana under state and/or federal laws. Due diligence is required.

FIN-2014-G001 includes this guidance on due diligence:

Providing Financial Services to Marijuana-Related Businesses

This FinCEN guidance clarifies how financial institutions can provide services to marijuana-related businesses consistent with their BSA obligations. In general, the decision to open, close, or refuse any particular account or relationship should be made by each financial institution based on a number of factors specific to that institution. These factors may include its particular business objectives, an evaluation of the risks associated with offering a particular product or service, and its capacity to manage those risks effectively. Thorough customer due diligence is a critical aspect of making this assessment.

In assessing the risk of providing services to a marijuana-related business, a financial institution should conduct customer due diligence that includes: (i) verifying with the appropriate state authorities whether the business is duly licensed and registered; (ii) reviewing the license application (and related documentation) submitted by the business for obtaining a state license to operate its marijuana-related business; (iii) requesting from state licensing and enforcement authorities available information about the business and related parties; (iv) developing an understanding of the normal and expected activity for the business, including the types of products to be sold and the type of customers to be served (e.g., medical versus recreational customers); (v) ongoing monitoring of publicly available sources for adverse information about the business and related parties; (vi) ongoing monitoring for suspicious activity, including for any of the red flags described in this guidance; and (vii) refreshing information obtained as part of customer due diligence on a periodic basis and commensurate with the risk. With respect to information regarding state licensure obtained in connection with such customer due diligence, a financial institution may reasonably rely on the accuracy of information provided by state licensing authorities, where states make such information available.

As part of its customer due diligence, a financial institution should consider whether a marijuana-related business implicates one of the Cole Memo priorities or violates state law. This is a particularly important factor for a financial institution to consider when assessing the risk of providing financial services to a marijuana-related business. Considering this factor also enables the financial institution to provide information in BSA reports pertinent to law enforcement's priorities. A financial institution that decides to provide financial services to a marijuana-related business would be required to file suspicious activity reports ("SARs") as described below.

Please see the full text of *FIN-2014-G001 BSA Expectations Regarding Marijuana-Related Businesses* for additional guidance on such topics as:

- Marijuana laws and law enforcement priorities (the "Cole Memo" priorities);
- Filing suspicious activity reports on marijuana-related businesses, and red flags to distinguish priority SARs; and
- Currency Transaction Reports.

Due diligence & money services businesses (MSBs)

Regulators have special BSA/AML compliance expectations for credit unions serving MSBs. MSB is a term used by financial regulators to describe a business that isn't a bank or credit union but that provides some bank-like services, including currency dealers or exchangers, check cashers, issuers or sellers of traveler's checks or money orders, money transmitters, and providers or sellers of prepaid access.

If your credit union serves MSBs, then the NCUA expects it to consider, monitor, and mitigate the risks by developing policies, procedures, and processes to achieve certain goals. After performing required CIP and CDD procedures, the credit union needs to :

- Confirm that member MSBs register with FinCEN, if applicable.
- Confirm that member MSBs comply with state or local licensing requirements, if applicable.
- Confirm the member MSB's agent status, if applicable.
- Conduct a basic BSA/AML risk assessment to document the level of risk associated with the MSB account.
- Conduct enhanced due diligence (in addition to the minimum due diligence steps) for MSB accounts if the credit union determines that they pose a higher level of money laundering or terrorist financing risk.

For details, see The League's *ii Release No. 0187 - BSA: Money Services Businesses*.

CDD: IDENTIFYING BENEFICIAL OWNERS OF LEGAL ENTITIES

(31 C.F.R. §1010.230)

FinCEN's BSA regulations require credit unions and other covered institutions (including banks) to have written, risk-based CDD procedures as part of their BSA/AML compliance programs.

There are two aspects to FinCEN's CDD requirements, and the previous section of this release covered the first one: Conducting ongoing CDD to understand the nature and purpose of member/customer relationships so that the credit union can develop a member/customer risk profile, monitor for suspicious activity, and conduct enhanced due diligence for high-risk customers/members.

This section of the release covers the second aspect of CDD compliance: The CDD beneficial owner rules. Under those rules, credit unions must have written procedures to identify "beneficial owners" – the people who own and control "legal entity customers" – organizations opening credit union accounts. Credit unions then must verify the identities of those beneficial owners. Additionally, credit unions must establish procedures for making and maintaining a record of all of the identification and verification information collected.

Exhibit I of this release provides FinCEN's Frequently Asked Questions regarding CDD. Please review those FAQs for important guidance on how to apply the CDD requirements.

"Legal entity customer"

These CDD beneficial owner rules only apply to "legal entity customers," a term that is defined to mean "a corporation, limited liability company, or other entity that is created by the filing of a public document with the Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account." In other words, the CDD beneficial owner rules apply to most organizations.

However, the definition does not include sole proprietorships, unincorporated associations (such as, scout troops and youth sports leagues), or natural persons opening accounts on their own behalf. The definition also exempts certain types of organizations, because information about their ownership and control is available from other sources:

- A department or agency of the federal, state, or local government;
- Any entity established under the federal, state or local laws of the U.S., or any interstate compact, that exercises governmental authority on behalf of the U.S. or of any such State or political subdivision;
- Any entity whose common stock is listed on one of the stock exchanges;
- Any subsidiary of an entity listed on one of the stock exchanges and whose common stock is owned (at least 51%) by the listed entity;
- An issuer of securities;
- An investment company;
- An investment advisor;
- An exchange or clearing agency;
- An entity registered with the Securities and Exchange Commission;
- An entity registered with the Commodity Futures Trading Commission;
- A bank holding company;
- A pooled investment vehicle;
- An insurance company regulated by a state;
- A financial market utility;
- A foreign financial institution, where its regulator maintains beneficial ownership information; and
- A non-U.S. governmental department, agency or political subdivision that engages only in governmental activities.

Trusts

A trust may or may not be subject to the CDD beneficial owner rules.

Sometimes, trusts are created for special business purposes. (Credit unions should note that the Wisconsin Trust Code does not apply to business trusts, as explained in *ii Release No. 0116*.) Business trusts are created by a filing with a state office. In Wisconsin a business trust (also called a statutory trust or a common law trust), is a trust created for the purpose of making profit and usually characterized by some kind of commercial activity and transferable certificates of interest. It is organized by creating a declaration of trust. In order to have authority to conduct business in Wisconsin, it must file an application with the DFI, accompanied by an original or certified copy of its declaration of trust. (Wis. Stats. Chap. 226.14.) Such a trust is a “legal entity” under the CDD rules

Other kinds of non-statutory trusts are much more common at credit unions. Usually called revocable, irrevocable or family trusts, these are contractual arrangements between the person who provides the funds or other assets and spells out the trust’s terms (the grantor) and the person with control over the assets (the trustee) for the benefit of someone (the beneficiaries). Forming a common revocable or irrevocable trust does not generally require any action by the state – so these trusts do not meet the definition of “legal entity” under the CDD rules. FinCEN recognizes that identifying a “beneficial owner,” as defined in the rule, from among these parties would be impossible.

But what if a trust owns (wholly or partially) the “legal entity customer” that is opening an account at the credit union? The rules says that where 25% or more of the equity interests of a legal entity are owned by a trust (other than a statutory trust), credit unions would collect and verify the identity of the trustee. In this case, the individual opening the account would still be the one required to provide the credit union with the beneficial owner information.

FinCEN also reminds credit unions that although they are not required to look through a trust to its beneficiaries, they “may need to take additional steps to verify the identity of a member that is not an individual, such as obtaining information about persons with control over the account.”

“d/b/a” accounts

Sole proprietorships are not “legal entities” and are not subject to the CDD beneficial owner rules. As explained in *ii Release No. 0161*, in a sole proprietorship, the owner is the business. No legal formalities are required to form a sole proprietorship; nothing needs to be filed with the state. Sole proprietorships have one owner, who manages all of the affairs of the business. A sole proprietor’s account should be titled in the individual owner’s name, and it can (but does not have to be) followed by d/b/a and his/her trade name. For example, a sole proprietor might open an account as “John Doe, d/b/a Expert Roofing.”

Credit unions sometimes assume that a “d/b/a” account is always a sole proprietorship, and they use the terms “d/b/a” and “sole proprietorship” interchangeably. This is not accurate. *Any* organization may also indicate that it is doing business under an assumed name. For example, a corporation might indicate “ABC Corp., d/b/a Quick Lube.” Whether an account includes a “d/b/a” trade name is irrelevant to determine whether it is subject to the CDD beneficial ownership rules.

“Beneficial Owners”

Whenever a “legal entity customer” (as the rules define that term) first opens an account, the credit union must identify its “beneficial owners.”

In 2026, FinCEN granted exceptive relief to covered financial institutions (see *FIN-2026-R001*) from the requirements of the rule, to identify and verify the identities of beneficial owners of legal entity customers at each new account opening. Rather than having to identify and verify a legal entity customer’s beneficial owners each time that customer opens an account, the credit union may instead limit its identification and verification of the identities of beneficial owners to the following circumstances:

- When a legal entity customer first opens an account with the credit union;
- Any time thereafter when the credit union has knowledge of facts that would reasonably call into question the reliability of beneficial ownership information previously obtained about the legal entity customer; and
- As needed based on the credit union's risk-based procedures for conducting ongoing customer due diligence.

The CDD rules have a two-pronged definition of “beneficial owner,” with an ownership prong and a control prong. Under this approach, the credit union must identify:

- Each individual (if any) who, directly or indirectly, owns 25% or more of the equity interests in the “legal entity customer” (although credit unions are permitted to set a lower percentage threshold if they wish, and they are encouraged to do so if the entity is considered higher-risk); *and*
- A single person who has significant responsibility to control the legal entity (including an executive officer or senior manager, such as a CEO, CFO, COO, managing member, general partner, president, vice president or treasurer) or any other person who regularly performs similar functions.

The same person(s) may be identified under both prongs.

If no individual owns 25% or more of the equity interests in the organization (or a lower percentage threshold if the credit union has chosen to set one), then the credit union can instead just identify a beneficial owner under the control prong (without having to identify any owners under the ownership prong).

The following types of groups are only subject to the control prong, and no one need be identified under the ownership prong:

- Any legal entity that is established as a non-profit corporation or a similar entity and has filed its organizational documents with the appropriate state authority.
- Any legal entity only to the extent that it opens a private banking account subject to BSA requirements.
- Any pooled investment vehicle that is not exempt.

“Account”

FinCEN defines “account” under the CDD rules to mean the same thing it does under the CIP rules: A formal banking relationship, including a deposit account, a transaction account (like checking), a credit account (such as a loan, credit card, or line of credit), or other extension of credit. The term also includes safe deposit box or other safekeeping services, or cash management, custodian, and trust services.

The term “account” does not include:

- A product or service where a formal banking relationship is not established, such as check-cashing, wire transfer, or sale of a check or money order;
- An account that a credit union acquires through an acquisition, merger, purchase of assets, or assumption of liabilities; or
- An account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974. (ERISA plan accounts are not subject to the CDD beneficial owner rules because, FinCEN said, “accounts established to enable employees to participate in retirement plans established under ERISA are of extremely low money laundering risk.”)

Identifying Beneficial Owners

A credit union can identify the beneficial owners of an organization in one of three ways:

1. By obtaining a “Certification of Beneficial Owner(s)” – a standard form that is included in the rules (as appendix A to 31 C.F.R. § 1010.230). The certification form is *available here on FinCEN’s website*.
2. By using the credit union’s own forms, as long as they meet the requirement in the rules.
3. By obtaining the required information through any other means – provided the person opening the account and providing the information certifies that it is accurate to the best of his/her knowledge.

Using the standard “Certification Regarding Beneficial Owners of Legal Entity Customers” form is optional. A credit union gains no additional protections from liability by using it.

The certification form can be filled out without a beneficial owner that meets the ownership prong, but in all cases there must be at least one beneficial owner who meets the control prong – such as a CEO, CFO, VP or other member of the senior management team or a person that regularly performs similar functions.

The number of individuals that satisfy this definition of “beneficial owner” may vary from one to five depending on the factual circumstances. The same person may meet the criteria for both ownership and control.

This form requires the person opening the account to provide their name and title, as well as the name, address, date of birth and identification number for the "beneficial owners" of the entity.

If your credit union chooses to use FinCEN's certification form, it must be completed by the person opening the new account on behalf of a legal entity. It must be a natural person authorized to open the account – it cannot be the entity itself. (If the credit union uses one of the other ways to identify the beneficial owners, then it must obtain the required information from the individual opening the account – provided the individual certifies the information to the best of his/her knowledge.)

The person authorized by the organization to open the account should be identified in an account opening resolution, such as The League's Depository Declaration and Agreement (WCUL #81075). In some cases, that authorized account opener may be a relatively low-level employee, not necessarily one of the owners of the organization. That is why FinCEN only requires certification to the best of the person's knowledge. The CDD beneficial ownership rules do not require the person to have "heightened knowledge threshold," nor does the certification have to be notarized or approved by the organization's board.

Updating beneficial owner information

The CDD rules do not require the credit union to continuously update each organization's beneficial ownership information. Instead, the rules call for a "snapshot" of the entity's beneficial owners when a legal entity customer first opens a new account with the credit union.

However, FinCEN does expect credit unions to update their beneficial ownership information whenever they detect relevant information about the entity in the course of regular monitoring. As explained by FinCEN, such "information could include, e.g., a significant and unexplained change in customer activity. It could also include information indicating a possible change in beneficial ownership, when such change might be relevant to assessing the risk posed by the customer. In any such event, it is appropriate to update the customer information accordingly."

"Legal entities" owned by other entities

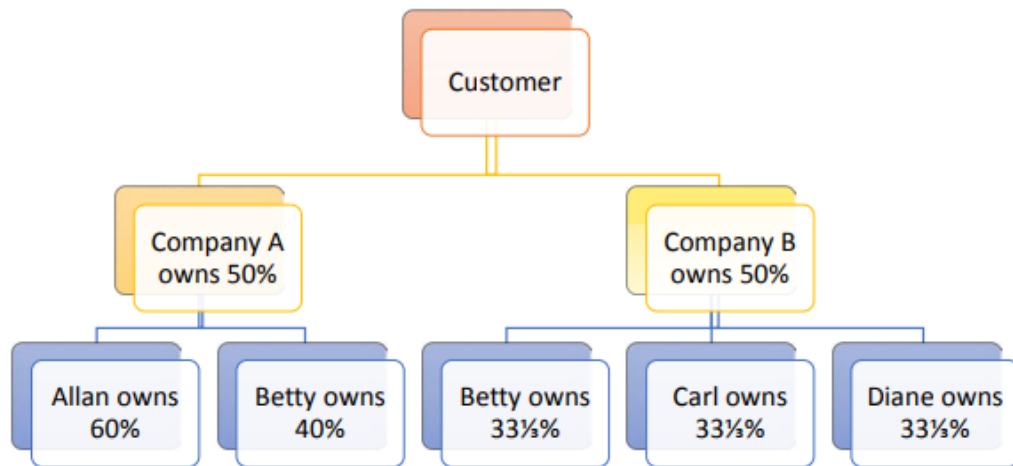
Sometimes, the legal entity opening an account is owned (completely or partially) by other legal entities. For example, an LLC that is joining the credit union may be owned by other LLCs, or by various other types of organizations, and/or by individuals. The CDD rules require the credit union to "drill down" and identify the beneficial owners of those other companies that own 25% or more the organization opening the account.

FinCEN's frequently asked questions about CDD (attached to this Release as Exh. I) address this issue:

When a legal entity is identified as owning 25 percent or more of a legal entity customer that is opening an account, is it necessary for a covered financial institution to request beneficial ownership information on the legal entity identified as an owner?

A. Under the Rule's beneficial ownership identification requirement, a covered institution must collect, from its legal entity customers, information about any individual(s) that are the beneficial owner(s) (unless the entity is excluded or the account is exempted). Therefore, covered financial institutions must obtain from their legal entity customers the identities of individuals who satisfy the definition, either directly or indirectly through multiple corporate structures, as illustrated in the following example.

For purposes of the Rule, Allan is a beneficial owner of Customer because he owns indirectly 30 percent of its equity interests through his direct ownership of Company A. Betty is also a beneficial owner of Customer because she owns indirectly 20 percent of its equity interests through her direct ownership of Company A plus $16\frac{2}{3}$ percent through Company B for a total of indirect ownership interest of $36\frac{2}{3}$ percent. Neither Carl nor Diane is a beneficial owner because each owns indirectly only $16\frac{2}{3}$ percent of Customer's equity interests through their direct ownership of Company B.



Verifying Identities of Beneficial Owners

After identifying an organization's "beneficial owners," the credit union must verify each of their identities, "according to risk-based procedures to the extent reasonable and practicable. At a minimum, these procedures must contain the elements required for verifying the identity of customers that are individuals under" CIP regulations.

In other words, a credit union must subject each beneficial owner to CIP. However, a credit union's CDD procedures for verifying the identities of beneficial owners do not have to be identical to its CIP procedures. For example:

- The credit union can obtain personally identifying information about each beneficial owner from the organization (not necessarily from the owners directly) as long as it has no reason to doubt that the information is reliable. The rules say: "A covered financial institution may rely on the information supplied by the legal entity customer regarding the identity of its beneficial owner or owners, provided that it has no knowledge of facts that would reasonably call into question the reliability of such information."
- The credit union can use photocopies or other reproductions of the documents. However, given the vulnerabilities in the reproduction process, each credit union is encouraged to conduct its own risk-based analyses of the types of photocopies and reproductions that it will accept, for example optical resolution threshold or digital reproductions transmitted in certain file formats.

Exemptions

The CDD beneficial owner rules include certain narrow exemptions, though they are not likely to apply to most organization accounts opened at credit unions. The requirements to identify and to verify the identities of an entity's beneficial owners do not apply when a financial institution opens an account for a legal entity that is:

- At the point-of-sale to provide credit products, including commercial private label credit cards, solely for the purchase of retail goods and/or services at these retailers, up to a limit of \$50,000;
- To finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of the postage products;
- To finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker;
- To finance the purchase or leasing of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

These exemptions do not apply, however, if the legal entity account member can make or receive payments from a 3rd party, or where a cash refund is possible.

Recordkeeping

Credit unions must have procedures for making and maintaining a record of all of the identification and verification information collected. At a minimum, those records must include:

- Any identification information obtained, including the standard certification form, if applicable;
- A description (type, identification number, place of issuance and dates of issuance and expiration, if any) of any document relied upon;
- Any non-documentary methods used; and
- Any measures taken in response to any substantive discrepancies, and the results those actions.

Identification-related records must be retained for 5 years after the date the account is closed.

Identity-verification-related records (i.e., CIP records) must be retained for 5 years after the record is made.

IOLTA Accounts

As explained in The League's *ii Release No. 0176*, Wisconsin law requires lawyers to maintain trust accounts under the state's Interest on Lawyers Trust Accounts (IOLTA) program if the lawyers hold pools of funds that belong to various clients or other third parties.

For purposes of the CDD rules, credit unions should treat the attorney opening an IOLTA account as the beneficial owner of the legal entity account. Similar to other guidance for IOLTA and escrow accounts, the attorney or escrow agent is considered the member and the credit union has no CIP obligations with respect to the underlying clients whose funds are being held in the IOLTA or escrow accounts.

Accounts Opened Before May 11, 2018

The CDD requirement to identify and verify beneficial owner information accounts only applies to accounts opened on or after May 11, 2018. FinCEN recognized that to implement these requirements retroactively would be "too unduly burdensome." That said, FinCEN does expect a credit union to obtain beneficial ownership information for accounts already in existence on May 11, 2018 when, in the course of normal monitoring, the credit union detects information relevant to reevaluating the account's risk.

FinCEN's Exemptive Relief from Beneficial Ownership Requirements for Legal Entity Customers of Rollovers, Renewals, Modifications, and Extensions of Certain Accounts

In a *September 7, 2018 ruling (FIN-2018-R004)*, FinCEN granted exemptive relief to covered financial institutions from the Beneficial Ownership Rule's requirement to identify and verify beneficial ownership information on or after May 11, 2018, as a result of the following:

- CD rollovers (as defined in FIN-2018-R004);
- loan renewals, modifications, and extensions (e.g., setting a later payoff date) that do not require underwriting review and approval;
- commercial line of credit or credit card account renewals, modifications, or extensions (e.g., setting a later payoff date) that do not require underwriting review and approval; and
- safe deposit box rental renewals.

For accounts with such rollover, renewal, modification or extension features opened after May 11, 2018, financial institutions must still collect the beneficial ownership information, as part of the account opening process. Financial institutions will no longer be required, however, to collect beneficial ownership information for these accounts at each rollover, renewal, extension, or modification for products described in FIN-2018-R004.

This relief does not apply to the initial opening of any of the types of accounts listed above, nor does it apply to relieve any covered financial institution of its other customer due diligence requirements under anti-money laundering program rules. Notwithstanding this permanent excepted relief, credit unions must comply with all other applicable AML requirements under the BSA, such as maintaining an AML program and reporting suspicious activity. [This exemptive relief replaced and superseded the May 16, 2018, 90-day limited exemptive relief, as well as the August 8, 2018, 30-day extension.](#)

Beneficial Owners & OFAC

As explained in The League's *ii Release No. 0148*, the U.S. Office of Foreign Assets Control (OFAC) maintains various lists of people, groups and nations that are subject to government sanctions. Credit unions must check the names of account-related parties and parties to transactions against the OFAC lists, and then block or reject transactions if they find a match.

FinCEN generally expects CDD beneficial ownership information to be treated like CIP and related information, and accordingly used to ensure that a credit union complies with other BSA-related requirements, such as OFAC. Credit unions should use beneficial ownership information to help ensure that they do not open or maintain an account, or otherwise engage in prohibited transactions or dealings involving individuals or entities subject to OFAC-administered sanctions.

In other words, credit unions should check the names of the beneficial owners against the OFAC lists.

Beneficial Owners & 314(a) Requests

As explained in The League's *ii Release No. 0071*, law enforcement agencies use FinCEN to gather information from financial institutions nationwide. FinCEN receives requests from law enforcement and upon review, passes on the requests to designated contacts within financial institutions across the country, including credit unions. These information requests are sometimes referred to as "314(a) requests" after the USA PATRIOT Act section that allows them. Credit unions generally receive 314(a) requests every two weeks. When a request comes in, a credit union must conduct a one-time search of its records to identify accounts or transactions of a named suspect.

When FinCEN published the CDD rules, it explained that it does not expect the beneficial owner provisions to add new requirements with respect to 314(a) requests. The 314(a) rule does not authorize the reporting of beneficial owner information associated with an account or transaction matching a named subject. Under that rule, credit unions need only search their records for account or transactions matching a named subject.

EXHIBITS – CUSTOMER DUE DILIGENCE TOOLS

- A – Procedure for Gathering Identity Information at Account Opening – Individuals (U.S. Citizen by Birth or Naturalization)
- B – Procedure for Gathering Identity Information at Account Opening – Individuals (Not a U.S. Citizen)
- C – Procedure for Gathering Identity Information at Account Opening – Organizations (Organized under U.S. Law)
- D – Procedure for Non-Documentary Verification
- E – CIP Guide
- F – Frequently Asked Questions about CIP
- G – CDD Risk Matrix for Individuals
- H – CDD Risk Matrix for Organizations
- I – FinCEN's Frequently Asked Questions Regarding CDD

* * * * *

League publications are designed to provide accurate information with regard to the subject matter covered, with the understanding that the League does not render legal services. If you have general questions regarding this release, please call The League at (608) 640-4050 if local; or (800) 242-0833. For specific legal advice, please consult your credit union's attorney.

Legal Affairs Department

KH/jb

© 2026 Wisconsin Credit Union League

EXHIBIT A - PROCEDURE FOR GATHERING IDENTITY INFORMATION AT ACCOUNT OPENING – INDIVIDUALS (U.S. CITIZEN BY BIRTH OR NATURALIZATION)

When a Customer asks to open a new Account, the Credit Union staff member handling the transaction shall gather enough information to establish a reasonable belief that the Credit Union knows the true identity of that Customer, using the steps below.

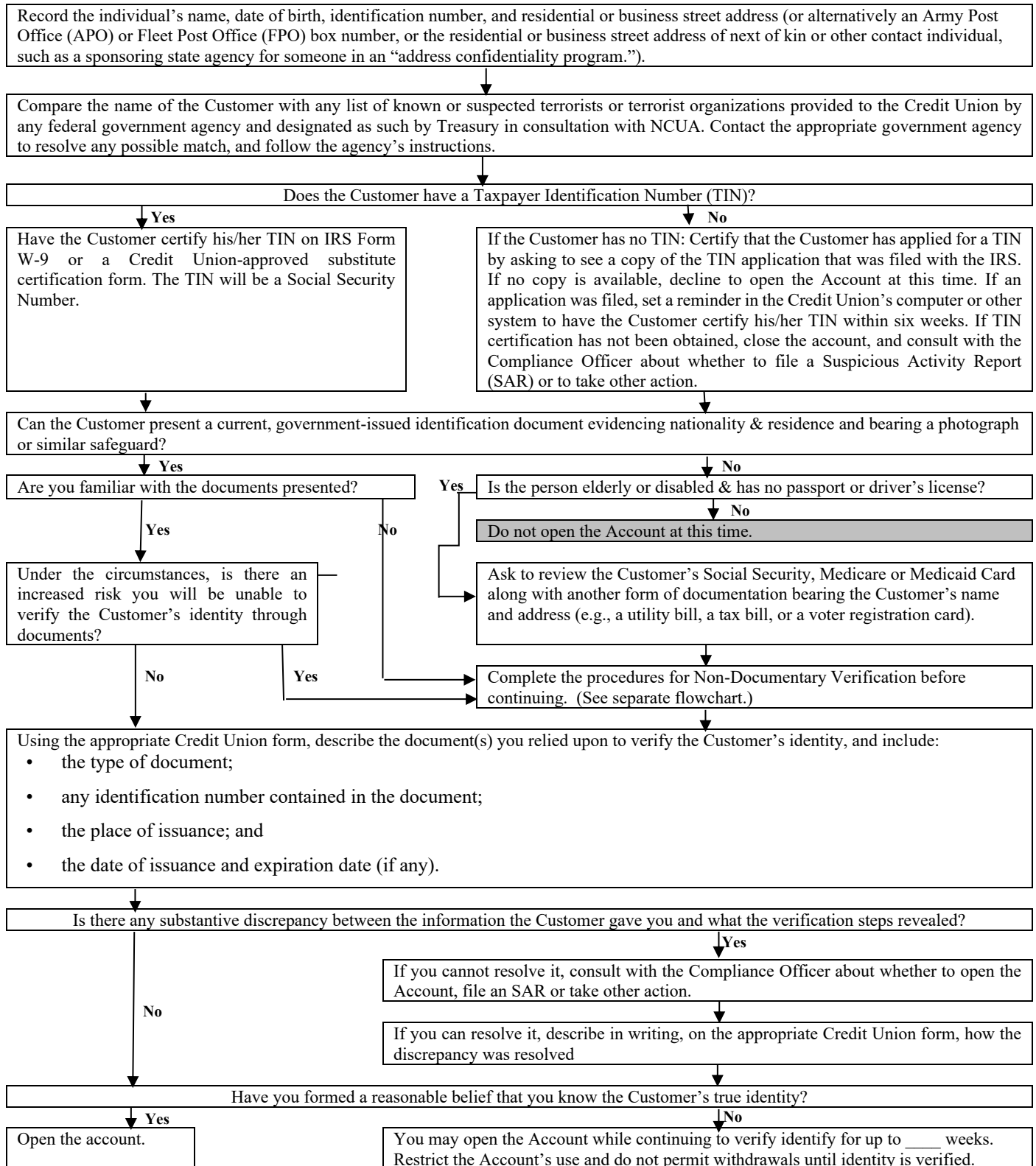


EXHIBIT B - PROCEDURE FOR GATHERING IDENTITY INFORMATION AT ACCOUNT OPENING – INDIVIDUALS (NOT A U.S. CITIZEN)

When a Customer asks to open a new Account, the Credit Union staff member handling the transaction shall gather enough information to establish a reasonable belief that the Credit Union knows the true identity of that Customer, using the steps below.

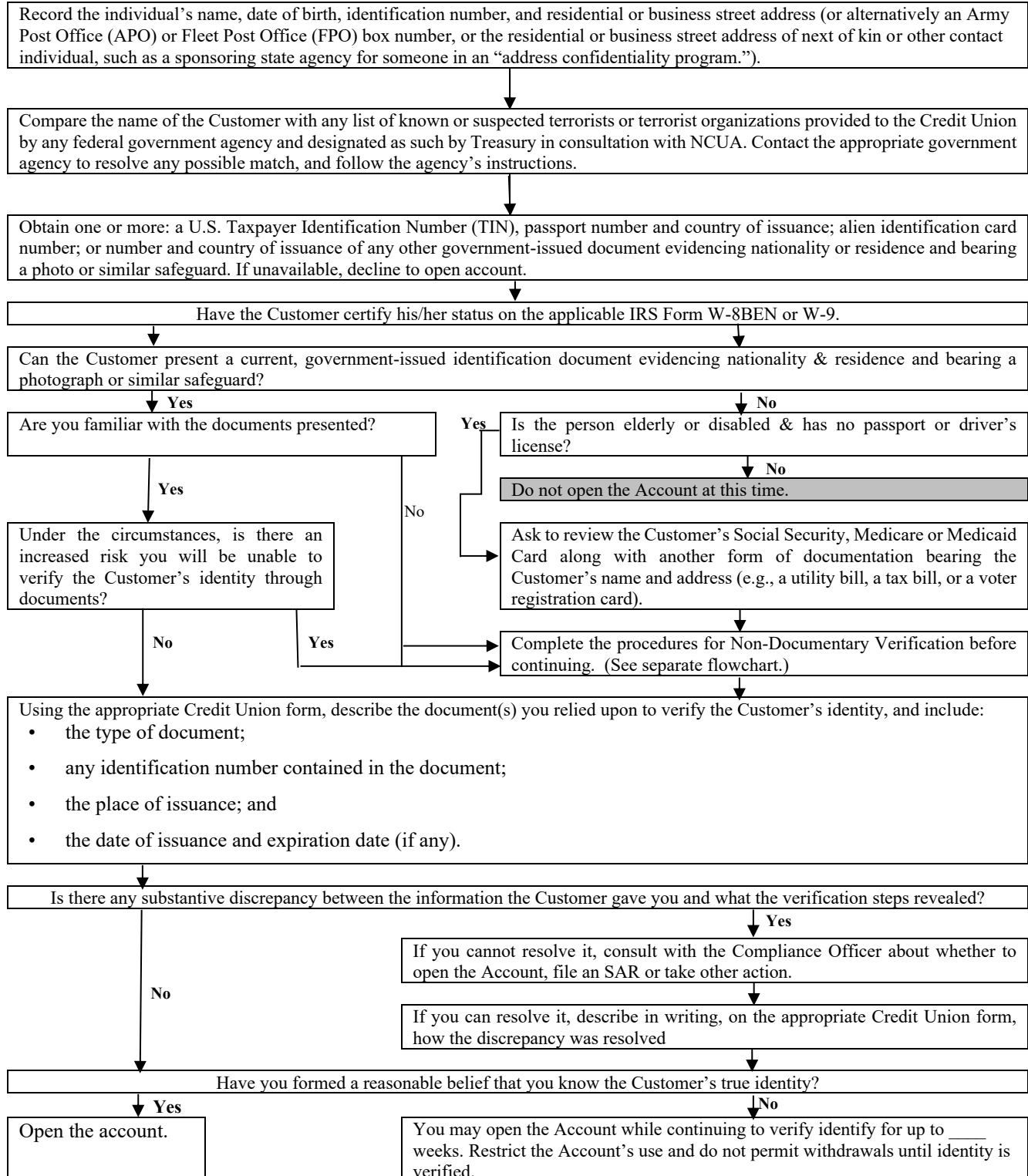


EXHIBIT C - PROCEDURE FOR GATHERING IDENTITY INFORMATION AT ACCOUNT OPENING – ORGANIZATION (ESTABLISHED OR/ORGANIZED UNDER U.S. LAW)

When a Customer asks to open a new Account, the Credit Union staff member handling the transaction shall gather enough information to establish a reasonable belief that the Credit Union knows the true identity of that Customer, using the steps below.

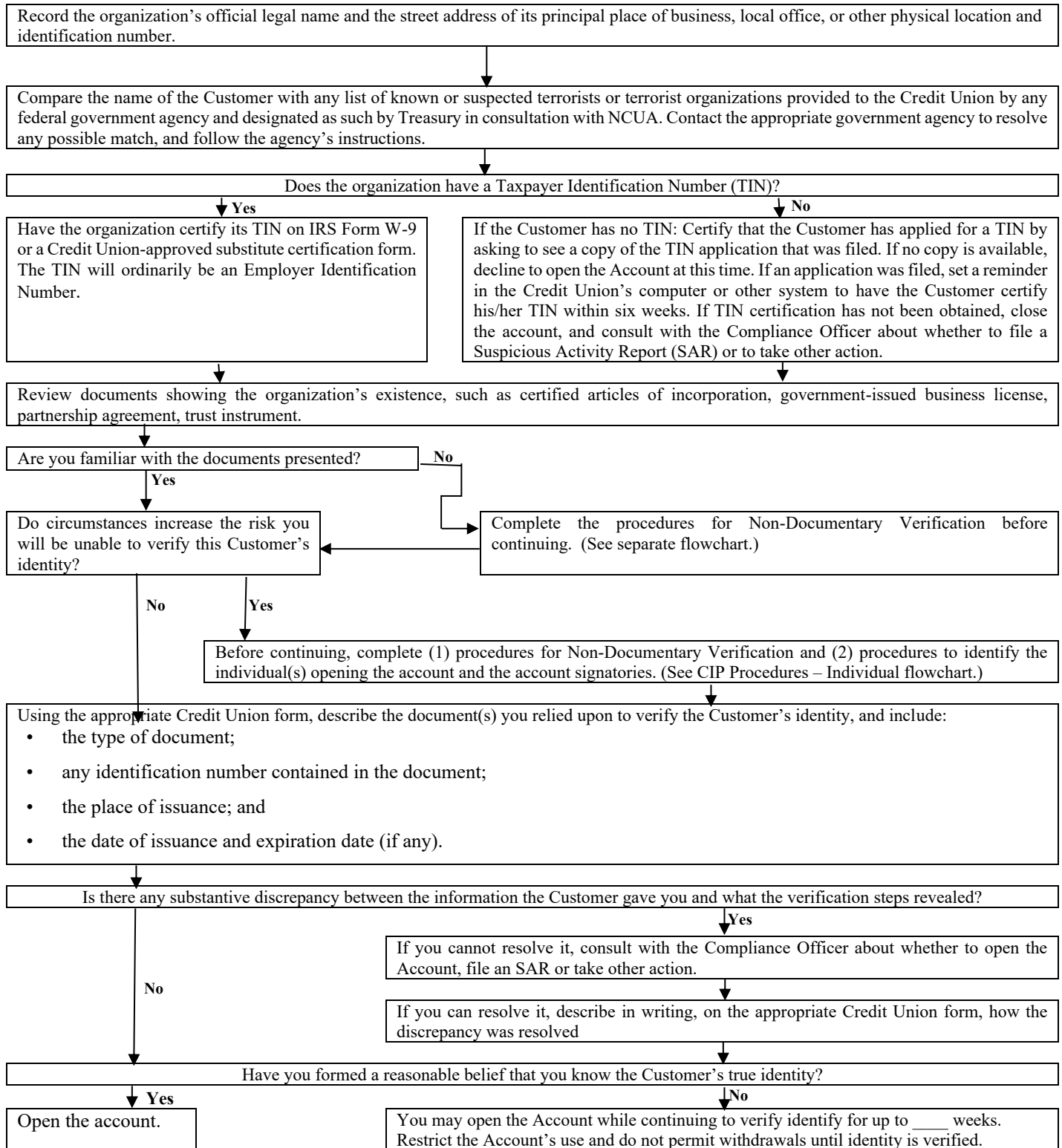


EXHIBIT D - PROCEDURE FOR NON-DOCUMENTARY VERIFICATION

For use:

- **when the member/customer cannot present a current government issued identification document with a photograph or similar safeguard, e.g., accounts opened by mail or Internet;**
- **when the Credit Union is unfamiliar or uncomfortable with the documentation evidence provided; or**
- **when the Credit Union policy dictates.**

When a Customer asks to open a new Account, the Credit Union staff member handling the transaction shall gather enough information to establish a reasonable belief that the Credit Union knows the true identity of that Customer, using the steps below.

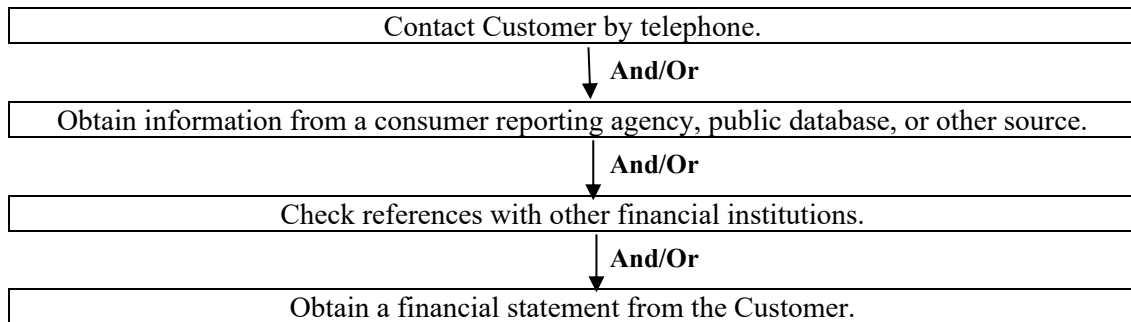


EXHIBIT E - CIP GUIDE

	U.S. Individual (an individual who is a U.S. citizen)	Non-U.S. Individual (an individual that does not meet the criteria of a U.S. Individual)	U.S. Non-Individual (an entity established or organized under the laws of a State or the U.S.)	Non-U.S. Non-Individual (an entity that does not meet the criteria of a U.S. Non-Individual)
Name	X	X	X	X
Address	Residence <i>(For an individual who does not have a street address, an APO or FPO box number, or the address of next of kin or of another contact individual. For individuals in a state's "address confidentiality program," use the address of the program's sponsoring agency.</i>	Residence	Principal place of business	Principal place of business
Date of Birth	X	X	N/A	N/A
Identification Number	U.S. taxpayer identification number (e.g., SSN or ITIN)	One or more of the following: - U.S. TIN (e.g., SSN or ITIN); - passport number and country of issuance; - alien identification card number; or - number & country of issuance of government-issued doc evidencing nationality or residence & bearing a photograph or similar safeguard.	EIN	One or more of the following: - U.S. TIN (e.g., EIN); or - number & country of issuance of government-issued doc evidencing nationality or residence & bearing a photograph or similar safeguard
Identity Verifying Documents (examples)	Unexpired government-issued ID evidencing nationality or residence & bearing a photo or similar safeguard, e.g.: - a driver's license; or - passport. <i>(For elderly or disabled who do not have the normally acceptable forms of ID, a Social Security, Medicare, or Medicaid card along with another document bearing their name & address (e.g., utility bill, tax bill, or voter registration card).</i>	Unexpired government-issued ID evidencing nationality or residence & bearing a photo or similar safeguard e.g.: - a driver's license; or - passport.	Documents showing the existence of the entity, such as: - certified articles of incorporation; - a government-issued business license; - partnership agreement; or - trust instrument.	Documents showing the existence of the entity, such as: - certified articles of incorporation; - a government-issued business license; - partnership agreement; or - trust instrument.

EXHIBIT F - FREQUENTLY ASKED QUESTIONS ABOUT CIP

The staff of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the United States Department of the Treasury (the Agencies) issued these frequently asked questions (FAQs) regarding the application of the joint regulation that implements section 326¹ of the USA PATRIOT Act and requires banks, savings associations, credit unions and certain non-federally regulated banks (bank) to have a Customer Identification Program (CIP).

While the purpose of the FAQs document is to provide interpretive guidance with respect to the CIP rule, the Agencies recognize that this document does not answer every question that may arise in connection with the rule. The Agencies encourage banks to use the basic principles set forth in the CIP rule, as articulated in these answers, to address variations on these questions that may arise, and expect banks to design their own programs in accordance with the nature of their business.

The Agencies emphasize that a bank's CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. It is critical that each bank develop procedures to account for all relevant risks, including those presented by the types of accounts maintained by the bank, the various methods of opening accounts provided, the type of identifying information available, and the bank's size, location, and type of business or customer base. Thus, specific minimum requirements in the rule, such as the four basic types of information to be obtained from each customer, should be supplemented by risk-based verification procedures, where appropriate, to ensure that the bank has a reasonable belief that it knows each customer's identity.

The Agencies note that the CIP, while important, is only one part of a bank's BSA/AML compliance program. Adequate implementation of a CIP, standing alone, will not be sufficient to meet a bank's other obligations under the BSA, regulations promulgated by its primary Federal regulator, such as Suspicious Activity Reporting requirements, or regulations promulgated by the Office of Foreign Assets Control.

Finally, these FAQs have been designed to help banks comply with the requirements of the CIP rule. They do not address the applicability of any other Federal or state laws.

References to specific citations have been adjusted within this release to reflect the reorganization of 31 C.F.R.103 to 31 C.F.R. Chapter X, effective March 1, 2011.

31 C.F.R. § 1020.100(a)(1) -- Definition of "account"

1. The CIP rule applies to a "customer," which is generally "a person that *opens* a new account." (Emphasis added.) At what point does the CIP rule apply when the account is a loan? When is the account opened?

"Customer" does not include a person who does not receive banking services, such as a person whose loan application is denied. See 68 FR 25090, 25093 (May 9, 2003). Therefore, when the account is a loan, the account is opened when the bank enters into an enforceable agreement to provide a loan to the customer. (January 2004)

2. Are loan participations purchased from third parties and loans purchased from a car dealer or mortgage broker within the exclusion from the definition of "account" for loans acquired through an acquisition, merger, purchase of assets, or assumption of liabilities?

Yes, this exclusion is intended to cover loan participations purchased from third parties and loans purchased from a car dealer or mortgage broker. If, however, the bank is extending credit to the borrower using a car dealer or mortgage broker as its agent, then it must ensure that the dealer or broker is performing the bank's CIP. (January 2004)

3. Are data processing, data warehousing, and data transmission on behalf of a person an "account?"

"Account" is defined to mean "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit. Account also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash

¹ Section 326 of the Act adds a new subsection (1) to 31 U.S.C. § 5318 of the Bank Secrecy Act ("BSA").

management, custodian and trust services.” The examples provided in 31 C.F.R. § 1020.100(a)(1) of formal banking relationships included within the meaning of “account” focus on bank products and services that relate to the deposit,

lending or custody of funds or other assets on behalf of a customer. Data processing, warehousing, and transmission services generally do not involve a service, dealing, or financial transaction that, taken alone, constitutes a “formal banking relationship” within the meaning of 31 C.F.R. § 1020.100(a)(1). If, however, any of these services are part of the establishment of a formal banking relationship, then the CIP rule in 31 C.F.R. § 1020.220 would apply. (April 2005)

31 C.F.R. § 1020.100(b)(1) -- Definition of “bank”

1. Is the CIP rule applicable to a bank’s foreign subsidiaries?

No. The CIP rule does not apply to any part of the bank located outside of the United States. Nevertheless, as a matter of safety and soundness, banks are encouraged to implement an effective CIP throughout their operations, including in their foreign offices, except to the extent that the requirements of the rule would conflict with local law. (January 2004)

2. Is the CIP rule applicable to bank holding companies and their non-bank subsidiaries, or to savings and loan holding companies and their non-savings association subsidiaries?

No, the CIP rule in 31 C.F.R. § 1020.220 applies only to a “bank.” A bank holding company is not subject to the rule solely because it owns a bank. However, a bank holding company may be subject to another CIP rule. For example, if the company is a broker-dealer in securities, it would be subject to 31 C.F.R. § 1023.220.

Similarly, a non-bank subsidiary of a bank holding company is not subject to the CIP rule for banks solely as a result of being affiliated with a bank in a holding company structure. However, a non-bank subsidiary may be subject to one of the other CIP rules.

Even if a bank holding company is not itself subject to the CIP rule under 31 C.F.R. § 1020.220, it should, as a matter of safety and soundness, take appropriate measures throughout its organization to ensure that each entity is in compliance with any applicable CIP rule, to ensure that new accounts receive appropriate due diligence, and generally to protect the consolidated organization from risks associated with money laundering and financial crime.

The analysis set forth above is equally applicable to savings and loan holding companies and their non-savings association subsidiaries. (April 2005)

3. Should subsidiaries of a bank implement a customer identification program?

Yes. The Federal banking agencies take the position that implementation of customer identification programs by subsidiaries of banks is appropriate as a matter of safety and soundness and protection from reputational risks. Subsidiaries (other than functionally regulated subsidiaries) of banks should comply with the customer identification program rule that applies to the parent bank when opening an account within the meaning of 31 C.F.R. § 1020.220. In addition, a number of the Federal banking agencies have separately issued rules that require certain subsidiaries of banks to conduct their activities pursuant to the same terms and conditions that apply to the conduct of such activities by the parent bank. See, e.g., 12 C.F.R. § 5.34 (OCC); 12 C.F.R. § 559.3(h) (OTS).

Some functionally regulated subsidiaries of banks are already subject to a customer identification program rule issued jointly by their functional regulator and FinCEN (i.e., 31 C.F.R. § 1023.220 (broker-dealers); 31 C.F.R. § 1024.220 (mutual funds); and 31 C.F.R. § 1026.220 (futures commission merchants and introducing brokers)). For purposes of the requirements imposed under section 326 of the USA PATRIOT Act, functionally regulated subsidiaries are: broker-dealers, investment companies, investment advisers registered with the SEC, persons licensed to provide insurance, and any entity with respect to a financial activity that is subject to the jurisdiction of the CFTC (such as futures commission merchants, introducing brokers, commodity trading advisors, commodity pools, and commodity pool operators). See 31 U.S.C. § 5318(l)(4); 15 U.S.C. §§ 6805, 6809. Subsidiaries of banks that are functionally regulated by the SEC or the CFTC are required to comply with the applicable CIP rules issued by the SEC or CFTC, respectively, and FinCEN.

The Federal banking agencies, SEC, CFTC, Department of the Treasury, and FinCEN have worked together to create uniform rules that minimize potential conflicts or differences between the agencies’ rules. In addition, Treasury and FinCEN intend to issue customer identification program rules applicable to other types of financial institutions in the future. (April 2005)

31 C.F.R. § 1020.100(c)(1) -- Definition of “customer”

1. Who is the “customer” when an account is opened by an individual who has power-of- attorney for a competent person who is the named owner of the account?

The CIP rule provides that a “customer” generally is “a person that opens a new account.” 31 C.F.R. § 1020.100(c)(1)(i). When an account is opened by an individual who has power-of-attorney for a competent person, the individual with a power-of-attorney is merely an agent acting on behalf of the person that opens the account. Therefore, the “customer” will be the named owner of the account rather than the individual with a power-of-attorney over the account. By contrast, an individual with power-of-attorney will be the “customer” if the account is opened for a person who lacks legal capacity. 31 C.F.R. § 1020.100(c)(1)(ii)(A). (January 2004)

2. Is a person who becomes co-owner of an existing deposit account a “customer” to whom the CIP rule applies?

Yes, a person who becomes the co-owner of an existing deposit account is a “customer” subject to the CIP rule because that person is establishing a new account relationship with the bank. (January 2004)

3. Is a new borrower who is substituted for an existing borrower through an assumption of a loan a “customer” to whom the CIP rule applies?

Yes, a new borrower who is substituted for an existing borrower through an assumption of a loan is a “customer” because the new borrower is establishing a new account relationship with the bank. (January 2004)

4. The CIP rule requires a bank to verify the identity of each “customer.” Under the CIP rule, a “customer” generally is defined as “a person that opens a new account.” If a pension plan administrator chooses to remove a former employee from the plan pursuant to section 657(c) of the Economic Growth and Tax Relief Reconciliation Act of 2001 (EGTRRA), it is required by law to transfer these funds to a financial institution. In addition, an administrator of a terminated plan may remove former employees that it is unable to locate, by transferring their benefits to a financial institution. Would a plan administrator or the former employee be a bank “customer” where funds are transferred to a bank and an account established in the name of the former employee, in either of these situations?

In either situation, the administrator has no ownership interest in or other right to the funds, and therefore, is not the bank’s “customer.” Nor would we view the administrator as acting as the customer’s agent when the administrator transfers the funds of former employees in these situations. A customer relationship arises and the requirements of the rule are implicated when the former employee “opens” an account. While the former employee has a legally enforceable right to the funds that are transferred to the bank, the employee has not exercised that right until he or she contacts the bank to assert an ownership interest. Thus, in light of the requirements imposed on the plan administrator under EGTRRA, as well as the requirements in connection with plan terminations, the former employee will not be deemed to have “opened a new account” for purposes of the CIP rule until he or she contacts the bank to assert an ownership interest over the funds, at which time a bank will be required to implement its CIP with respect to the former employee.

This interpretation applies only to (1) transfers of funds as required under section 657(c) of EGTRRA, and (2) transfers to banks by administrators of terminated plans in the name of participants that they have been unable to locate, or who have been notified of termination but have not responded, and should not be construed to apply to any other transfer of funds that may constitute opening an account. (January 2004)

5. A bank is an agent for a (bank) credit card issuer. The cards are co-branded, the two banks share in the revenue from the cards issued. However, the issuer approves the credit card applications and handles collections. Is a person who obtains a credit card a customer of the agent bank or the card issuer?

A person who receives a credit card is receiving an extension of credit from, and therefore is establishing an account with, the issuing bank. The agent bank is compensated by the issuing bank and not by the customer. For these reasons, the issuing bank is responsible for ensuring that its CIP applies to the customer. However, the agent bank may perform parts of the CIP on behalf of the issuing bank. As with any other responsibility performed by an agent, the issuing bank ultimately is responsible for the agent’s compliance with the requirements of the CIP rule. See 68 FR 25090, 25104 (May 9, 2003). Alternatively, the issuing bank may *rely* upon the agent bank to perform elements of its CIP, provided that the issuing bank

is able to satisfy the requirements of the reliance provision, 31 C.F.R. § 1020.220(a)(6), including the requirement that the person be a customer of both the issuing and agent bank. (January 2004)

6. Does the CIP rule prohibit a minor from opening an account?

No, the CIP rule does not bar a minor from opening an account. It merely states that the bank's "customer" is the individual who opens the account for an individual who lacks legal capacity, such as a minor. In other words, if a parent opens an account for a minor, the bank's customer is the parent. If, however, a minor opens the account, then the minor is the bank's customer. For example, where a bank sends its employees to elementary schools so that students may open savings accounts as part of a program to promote financial literacy, a student opening an account is the bank's customer. In this situation, as for all customers, the bank should get the name, address, date of birth, and taxpayer identification number of the student. Since verification procedures are risk-based, banks can use any reasonable documentary or non-documentary method to verify a student's identity. In this case, the bank might verify a student's identity using a student identification card or by having the student's teacher confirm the student's identity. (April 2005)

7. The definition of "account" excludes accounts opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974 (ERISA). In the case of a trust, custodial, or other administrative account established by an employer at a bank to maintain and administer assets under a non-ERISA employee retirement, benefit, or deferred compensation plan, who is the bank's "customer?" Is a participant in or beneficiary of such an account the "customer?"

In the case of these accounts (including, for example, accounts established by governmental entities to administer retirement or benefit plans or by employers to administer stock option or restricted stock plans) that are established as trusts, the bank's "customer" will be the trust established by the employer to maintain the assets. If the account is not a trust, the bank's "customer" will be the employer that contracts with the bank to establish the account.* Based on the bank's risk assessment of any new account opened by a customer that is not an individual, the bank may need "to obtain information about" individuals with authority or control over such an account, including signatories, in order to verify the customer's identity. See 31 C.F.R. § 1020.220(a)(2)(ii)(C).

For purposes of the CIP rule, a participant in or beneficiary of such an account will not be deemed to be the bank's "customer," as such a person will not have initiated the relationship with the bank. The account will not be considered opened by the employee even if a subaccount is maintained in the employee's name, or the employee is able to make deposits into the account, so long as such ability to make deposits is limited to rolling over assets from another plan, purchasing securities or exercising options to purchase securities issued by the employer, or repaying a loan, in accordance with the terms of the plan. By contrast, where an *individual* opens an individual retirement account in a bank, the individual who opens the account is the bank's "customer." (April 2005)

* Note, however, that the CIP rule will not apply if the employer is exempt from the definition of "customer" under 31 C.F.R. § 1020.100(c).

8. Does the definition of "customer" include the relationship with an investor that is established when a bank acts as a registered transfer agent for an issuer, for example, when it effects transactions for the investor in the securities of an issuer as part of the issuer's dividend reinvestment plan or as part of the plan or program for the purchase or sale of that issuer's shares in a manner that does not cause the bank to be a broker under the Securities Exchange Act of 1934?

No. A bank that is a registered transfer agent is acting as agent of the issuer of securities. The relationship with the investor does not constitute a "formal banking relationship established to engage in services, dealings, or other financial transactions" with the investor in these situations. Thus, the bank's relationship with the investor does not constitute a "customer" relationship. With respect to a bank acting as a transfer agent for its own securities, such bank is dealing with shareholders as shareholders and not as customers. (April 2005)

9. Who is the "customer" for purposes of trust accounts? Does it make a difference whether the bank or a third party is trustee for the trust?

In the case of a trust account, the "customer" is the trust whether or not the bank is the trustee for the trust. "A bank will not be required to look through trust, escrow, or similar accounts to verify the identities of beneficiaries and instead will only be

required to verify the identity of the named accountholder.” See 68 FR 25090, 25094 (May 9, 2003). However, the CIP rule also provides that, based on the bank’s risk assessment of a new account opened by a customer that is not an individual, the bank may need “to obtain information about” individuals with authority or control over such an account, including signatories, in order to verify the customer’s identity. See 31 C.F.R. § 1020.220(a)(2)(ii)(C). For example, in certain circumstances involving revocable trusts, the bank may need to gather information about the settlor, grantor, trustee, or other persons with the authority to direct the trustee, and who thus have authority or control over the account, in order to establish the true identity of the customer. (April 2005)

10. Who is the “customer” for purposes of escrow accounts?

An escrow account is an account generally established for the deposit of funds that are to be paid to a specified party on the fulfillment of escrow conditions or returned. If a bank establishes an account in the name of a third party, such as a real estate agent, who is acting as escrow agent, then the bank’s customer will be the escrow agent. If the bank is the escrow agent, then the person who establishes the account is the bank’s “customer.” For example, if the purchaser of real estate directly opens an escrow account and deposits funds to be paid to the seller upon satisfaction of specified conditions, the bank’s customer will be the purchaser. Further, if a company in formation establishes an escrow account for investors to deposit their subscriptions pending receipt of a required minimum amount, the bank’s customer will be the company in formation (or if not yet a legal entity, the person opening the account on its behalf). “A bank will not be required to look through trust, escrow, or similar accounts to verify the identities of beneficiaries and instead will only be required to verify the identity of the named accountholder.” See 68 FR 25090, 25094 (May 9, 2003). However, the CIP rule also provides that, based on the bank’s risk assessment of a new account opened by a customer that is not an individual, the bank may need “to obtain information about” individuals with authority or control over such an account, including signatories, in order to verify the customer’s identity. See 31 C.F.R. § 1020.220(a)(2)(ii)(C). (April 2005)

31 C.F.R. § 1020.100(c)(2)(iii) – Person with an existing account

1. A loan and a time deposit are each an “account” for purposes of the CIP rule. How do the requirements of the CIP rule apply to a loan that is renewed, or a certificate of deposit that is rolled over?

The CIP rule applies to a “customer,” generally, “a person that opens a *new* account.” 31 C.F.R. § 1020.100(c)(1)(ii). (Emphasis added.) “Account” means a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit. 31 C.F.R. § 1020.100(a)(1). For purposes of the CIP rule, each time a loan is renewed or a certificate of deposit is rolled over, the bank establishes another formal banking relationship and a *new* account is established. However, the rule provides that the term “customer” does not include a person that has an *existing* account with the bank, provided that the bank has a reasonable belief that it knows the true identity of the person. 31 C.F.R. § 1020.100(c)(2)(iii). In each of these cases, the customer has an *existing* account. Therefore, as long as the bank has a reasonable belief that it knows the person’s true identity, the bank need not perform its CIP when a loan is renewed or certificate of deposit is rolled over. However, if a new customer is added to the loan or deposit account, the bank would need to satisfy the CIP rule with respect to that new account relationship. (January 2004)

2. Does the exclusion from the definition of “customer” in 31 C.F.R. § 1020.100(c)(2)(iii) for a person with an existing account extend to a person who has had an account with the bank in the last twelve months but who no longer has an account?

No, this provision only excludes from the definition of “customer” a person that at the time a new account is opened currently “has an existing account with the bank,” and only if the bank has a reasonable belief that it knows the true identity of the person. Therefore, for example, when a person has a deposit account and subsequently obtains a loan, the person has an existing account with the bank. Conversely, a person would not be deemed to have an existing account at the bank if the person had a loan, paid it off, and twelve months later obtains a new loan. (January 2004)

3. How can a bank demonstrate that it has “a reasonable belief that it knows the true identity of a person with an existing account” with respect to persons that had accounts with the bank as of October 1, 2003?

Among the ways a bank can demonstrate that it has “a reasonable belief” is by showing that prior to the issuance of the final CIP rule, it had comparable procedures in place to verify the identity of persons that had accounts with the bank as of October 1, 2003, though the bank may not have gathered the very same information about such persons as required by the final CIP rule. Alternative means include showing that the bank has had an active and longstanding relationship with a particular person, evidenced by such things as a history of account statements sent to the person, information sent to the IRS about the person’s accounts without issue, loans made and repaid, or other services performed for the person over a period of time. This alternative, however, may not suffice for persons that the bank has deemed to be high risk. (January 2004)

4. Can a bank exclude from the definition of “customer” a person that has an existing account with its affiliate?

No, a person that has an existing account with a bank affiliate does not qualify as “a person who has an existing account with the bank” within the meaning of 31 C.F.R. § 1020.100(c)(2)(iii). However, the bank may be able to *rely* on its affiliate to perform elements of its CIP, as provided in 31 C.F.R. § 1020.220(a)(6). (January 2004)

31 C.F.R. § 1020.220(a)(2)(i) -- Information required

1. What address should be obtained for customers who live in rural areas who do not have a residential or business address or the residential or business address of next of kin or another contact individual? For example, is a rural route number acceptable?

Yes, the number on the roadside mailbox on a rural route is acceptable as an address. A rural route number, unlike a post office box number, is a description of the approximate area where the customer can be located. In the absence of such a number, and in the absence of a residential or business address for next of kin or another contact individual, a description of the customer’s physical location will suffice. (January 2004)

2. Can a bank open an account for a U.S. person that does not have a taxpayer identification number?

No, the bank cannot unless the customer has applied for a taxpayer identification number, the bank confirms that the application was filed before the customer opened the account, and the bank obtains the taxpayer identification number within a reasonable period of time after the account is opened. Note, however, that a bank does not need to obtain a taxpayer identification number when opening a new account for a customer that has an existing account, as long as the bank has a reasonable belief that it knows the true identity of the customer. A bank may also open an account for a person who lacks legal capacity with the identifying information, including taxpayer identification number, of an individual who opens an account for that person. (January 2004)

3. The CIP rule requires a bank to obtain a taxpayer identification number from the customer prior to opening an account from a customer that is a U.S. person. When the bank’s customer is a trust, what taxpayer identification number should the bank obtain?

The taxpayer identification number for a trust is the trust’s employer identification number (EIN). If the trust is not required to have an EIN under the tax laws, then the bank may obtain the grantor’s taxpayer identification number, consistent with section 6109 of the Internal Revenue Code and the regulations thereunder. (April 2005)

31 C.F.R. § 1020.220(a)(2)(ii) -- Customer verification

1. Must a bank verify the accuracy of all of the identifying information it collects in connection with 31 C.F.R. § 1020.220(a)(2)(i)?

The final rule provides that a bank’s CIP must contain procedures for verifying the identity of the customer, “using the information obtained in accordance with paragraph (a)(2)(i),” namely the identifying information obtained by the bank. 31 C.F.R. § 1020.220(a)(2)(i). A bank need not establish the accuracy of every element of identifying information obtained but must do so for enough information to form a reasonable belief it knows the true identity of the customer. See 68 FR 25090, 25099 (May 9, 2003). (January 2004)

2. Can a bank use an employee identification card as the sole means to verify a customer’s identity?

A bank using documentary methods to verify a customer’s identity must have procedures that set forth the documents that the bank will use. The CIP rule gives examples of types of documents that have long been considered primary sources of

identification and reflects the Agencies' expectation that banks will obtain government-issued identification from most customers. However, other forms of identification may be used if they enable the bank to form a reasonable belief that it knows the true identity of the customer. Nonetheless, given the availability of counterfeit and fraudulently obtained documents, a bank is encouraged to obtain more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity. (January 2004)

3. Can a bank use an electronic credential, such as a digital certificate, as a non-documentary means to verify the identity of a customer that opens an account over the Internet or through some other purely electronic channel?

A bank may obtain an electronic credential, such as a digital certificate, as one of the methods it uses to verify a customer's identity. However, the CIP rule requires the bank to have a reasonable belief that it knows the true identity of the customer. Therefore, for example, the bank is responsible for ensuring that the third party uses the same level of authentication as the bank itself would use. See also FFIEC guidance titled "Authentication in an Electronic Banking Environment" (July 30, 2001). (January 2004)

4. How should a bank verify the identity of a partnership that opens a new account when there are no documents or non-documentary methods that will establish the identity of the partnership?

A bank opening an account for such a partnership must undertake additional verification by obtaining information about the identity of any individual with authority or control over the partnership account, in order to verify the partnership's identity, as described in 31 C.F.R. § 1020.220(a)(2)(ii)(C). (January 2004)

5. How should a bank verify the identity of a sole proprietorship that opens a new account, (such as an account titled in the name of an individual "doing business as" a sole proprietorship) when there are no documents or non-documentary methods that will establish the identity of the sole proprietorship?

In some states, sole proprietorships are required to file "fictitious" or "assumed name certificates." Banks may choose to use these certificates as a means to verify the identity of a sole proprietorship, if appropriate. However, when there are no documents or non-documentary methods that will establish the identity of the sole proprietorship, the bank must undertake additional verification by obtaining information about the sole proprietor or any other individual with authority or control over the sole proprietorship account -- such as the name, address, date of birth, and taxpayer identification number of the sole proprietor, or any other individual with authority or control over the account -- in order to verify the sole proprietorship's identity, as described in 31 C.F.R. § 1020.220(a)(2)(ii)(C). (January 2004)

31 C.F.R. § 1020.220(a)(3) – Required records

1. Would it be acceptable to retain a description of the non-documentary customer verification method used (such as a consumer credit report or an inquiry to a fraud detection system) in a general policy or procedure instead of recording the fact that a particular method was used on each individual customer's record?

Yes, provided that the record cross-references the specific provision(s) of the risk-based procedures contained in the bank's CIP used to verify the customer's identity. (January 2004)

2. Can a bank keep copies of documents provided to verify a customer's identity, in addition to the description required under 31 C.F.R. § 1020.220(a)(3)(i)(B), even if it is not required to do so?

Yes, a bank may keep copies of identifying documents that it uses to verify a customer's identity. A bank's verification procedures should be risk-based and, in certain situations, keeping copies of identifying documents may be warranted. In addition, a bank may have procedures to keep copies of documents for other purposes, for example, to facilitate investigating potential fraud. (These documents should be retained in accordance with the general recordkeeping requirements in 31 C.F.R. § 1010.430.) Nonetheless, a bank should be mindful that it must not improperly use any document containing a picture of an individual, such as a driver's license, in connection with any aspect of a credit transaction. (January 2004)

31 C.F.R. § 1020.220(a)(3)(ii) – Retention of records

1. Does the original information obtained during account opening have to be retained or can the bank satisfy the recordkeeping requirement by just keeping updated information about the customer, i.e., the customer's current address?

The CIP rule requires that a bank retain the identifying information obtained about the customer *at the time of account opening* for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant. 31 C.F.R. § 1020.220(a)(3)(ii). Updated information serves valuable, but different, purposes. (January 2004)

2. If the bank requires a customer to provide more identifying information than the minimum during the account opening process, does it have to keep this information for more than five years?

The bank must keep for five years after the account is closed, or in the case of credit card accounts, five years after the account is closed or becomes dormant, all identifying information it gathers about the customer to satisfy the requirements of § 1020.220(a)(2)(i) of the CIP rule. 31 C.F.R. § 1020.220(a)(3)(ii). This would include any identifying information, the bank will use, at the time the account is opened, to establish a reasonable belief it knows the true identity of the customer. So, for example, if the bank obtains other identifying information at account opening in addition to the minimal information required, such as the customer's phone number, then the bank must keep that information. (January 2004)

3. How does the record retention period apply to a customer who simultaneously opens multiple accounts in the bank?

If several accounts are opened for a customer simultaneously, all identifying information about a customer obtained under 31 C.F.R. § 1020.220(a)(2)(i) must be retained for five years after the last account is closed or, in the case of credit card accounts, five years after the last account is closed or becomes dormant. All remaining records must be kept for five years after the records are made. (January 2004)

4. How does the record retention period apply to a situation where a bank sells a loan but retains the servicing rights to the loan?

When a bank sells a loan, the account is “closed” under the record retention provision (31 C.F.R. § 1020.220(a)(3)(ii)), regardless of whether the bank retains the servicing rights to the loan. Thus, a bank should keep the records of identifying information about a customer for five years after the date that the loan is sold, as required by 31 C.F.R. § 1020.220(a)(3)(ii). Any other record required by 31 C.F.R. § 1020.220(a)(3)(ii) must be kept for five years after the record is made. (April 2005)

31 C.F.R. § 1020.220(a)(4) -- Section 326 List

1. Has a list of known or suspected terrorists or terrorist organizations been designated for purposes of the CIP rule?

No such list has been designated to date. Banks will be contacted by their functional regulators when a list is issued. As of the time of publication, lists published by OFAC have not been designated as lists for purposes of the CIP rule. Of course, banks are separately obligated to check these lists in accordance with OFAC's regulations. (January 2004)

31 C.F.R. § 1020.220(a)(5) -- Customer notice

1. Does a bank have to provide notice to all owners of a joint account?

Yes, notice must be provided to all owners of a joint account. In addition, notice must be provided “in a manner reasonably designed to ensure that a customer is able to view the notice, or is otherwise given notice, before opening an account.” 31 C.F.R. § 1020.220(a)(5)(ii). The Agencies agree that a bank may satisfy this requirement by directly providing the notice to any one accountholder of a joint account for delivery to the other owners of the account. Similarly, the bank may open a joint account using information about each of the accountholders obtained from one accountholder, acting on behalf of the other joint accountholders. (January 2004)

2. How should a bank provide notice to its customer when it engages in indirect lending through a third party such as a mortgage broker or car dealer?

When a mortgage broker or car dealer is acting as the bank's agent in connection with a loan, the bank may delegate to its agent the obligation to perform the requirements of the bank's CIP rule. In contrast to the reliance provision in the CIP rule, the bank is ultimately responsible for its agent's compliance with the rule. Depending upon the manner in which the account is opened, the agent can provide notice to the bank's customer, for example, by posting a sign, printing the notice on the loan application given to the customer, orally providing the notice, or by providing the notice in any manner that is reasonably designed to ensure that the customer is given notice before opening an account. (January 2004)

31 C.F.R. § 1020.220(a)(6) -- Reliance

1. Where a bank is entitled to “rely” on another financial institution to perform its CIP, whose CIP must the relied-upon financial institution implement?

The reliance provision does not impose on the other financial institution the obligation to duplicate the procedures in the bank’s CIP. The reliance provision permits a bank to rely on another financial institution to perform any of the procedures of the bank’s CIP, meaning, any of the **elements** that the CIP rule requires to be in a bank’s CIP: (1) identity verification procedures, which include collecting the required information from customers and using some or all of that information to verify the customers’ identities; (2) keeping records related to the CIP; (3) determining whether a customer appears on a designated list of known or suspected terrorists or terrorist organizations; and (4) providing customers with adequate notice that information is being requested to verify their identities.

Note that a bank can only use the reliance provision when the other financial institution is regulated by a Federal functional regulator and is subject to a general BSA compliance program rule, they share the customer, the bank can show its reliance upon the other financial institution’s performance of an element of the bank’s CIP was reasonable under the circumstances, and the requisite contract is signed and certifications provided. (January 2004)

2. When a longstanding customer of another financial institution (including an affiliate) opens a new account at the bank, can a bank rely on the other financial institution’s verification of the identity of the customer performed before a CIP procedure was required?

A bank that is subject to the CIP rule may rely on another financial institution’s verification of the identity of the customer if the requirements of the reliance provision are satisfied. The bank would have to be able to demonstrate that such reliance upon the other financial institution’s verification of the identity of the customer is reasonable under the circumstances. For example, the bank could do so by reviewing the relied-upon institution’s procedures to ensure that they were adequate although the institution was not yet subject to a CIP rule when it verified the customer’s identity.

In addition, even when a bank is relying on the verification of identity performed by another institution, the bank would continue to be responsible for complying with all remaining requirements of the CIP rule, namely, the requirement that it keep records, provide customer notice, and as soon as a section 326 list has been designated, check the list when a new account is opened. (January 2004)

EXHIBIT G - CDD RISK MATRIX FOR INDIVIDUALS

The credit union needs to exercise customer due diligence (CDD) when opening accounts and monitoring existing accounts for suspicious activity. Gather information about account holders at account opening to determine risk, and reassess the risk rating if there is a change in the member's/customer's risk profile (e.g., expected account activity, change in employment or business operations, etc.). Apply enhanced due diligence to monitor activity of high-risk members/customers. Please review The League's ii Release No. 0159 and the FFIEC exam manual for details on CDD. The matrix below is offered only as a guide to help with risk-rating. It must be tailored to the credit union's operations. Because credit unions are each unique, and differ in their size, resources and staff, this matrix will not work for every credit union. Credit unions may consider assigning numerical scores to the various categories.

Account holder's name: _____

Account numbers: _____

Information Needed	Check all that apply
Length of CU membership	☐ Lower risk: 2+ years ☐ Medium risk: 1 to 2 years ☐ Higher risk: Less than 1 year
Account opening method	☐ Lower risk: In person with all account holders ☐ Medium risk: In person with some, but not all, account holders ☐ Higher risk: Not opened in person
Citizenship	☐ Lower risk: U.S. Citizen ☐ Higher risk: Non-U.S. citizen
Address	☐ Lower risk: Local ☐ Medium risk: Non-local but within U.S. ☐ Higher risk: Outside U.S.
Geographic location	Consider the location, residence or citizenship of the account's principals or beneficiaries and the location that is the source of account funds. The following are higher-risk: ☐ Country subject to OFAC sanctions or otherwise considered higher-risk, such as money laundering centers, supporters of terrorism, offshore financial centers, countries subject to FinCEN advisories, etc. ☐ High-intensity drug trafficking area (including Milwaukee, Waukesha, Racine, Kenosha, Rock, Brown and Dane counties in Wisconsin) www.whitehousedrugpolicy.gov/hidta/ ☐ High-intensity financial crimes area (including the Chicago area, New York, New Jersey, southern Florida, northern and southern California, the southwestern U.S. border region, Puerto Rico and the Virgin Islands) www.fincen.gov/law_enforcement/hifca/
Employment	☐ Lower risk: Employed locally in non-high-risk business; retired from non-high-risk business; student; or unemployed ☐ Medium risk: Self-employed; not employed locally; or retired from high-risk business ☐ Higher risk: Employed internationally; employment unknown; employed in high-risk business The following are considered higher risk businesses: ☐ Non-governmental organizations and charities (foreign and domestic) ☐ Non-bank financial institutions (e.g., check cashers, money services businesses) ☐ Casinos and card clubs ☐ Leather goods stores ☐ Car, boat and plane dealerships ☐ Used car or truck dealers and machine parts manufacturers ☐ Travel agencies ☐ Brokers/dealers in securities ☐ Jewel, gem, and precious metal dealers ☐ Auctioneers and pawn brokers ☐ Professional service providers (e.g., attorneys, accountants, doctors and real estate brokers)

Employment (cont'd)	☐ Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages) ☐ Ship, bus, plane operators ☐ Telemarketers ☐ Deposit brokers ☐ Import/export companies ☐ Offshore businesses or banks
CTR/SAR filings	☐ Lower risk: Account holder has no previous CTR or SAR filings ☐ Higher risk: Account holder has previous CTR or SAR filings and should be given an overall risk rating of "high"
Account type	☐ Lower risk: Savings; checking (1 or 2 joint owners); IRA; share certificate ☐ Medium risk: Guardianship; custodial/UTMA; checking (3 or more joint owners); auto loan; mortgage; HELOC; signature loan; credit card ☐ Higher risk: Irrevocable trust; power of attorney; construction loan
Types of transactions	☐ Lower risk: Occasional currency deposits / withdrawals over \$3,000; internet banking / bill pay; ACH receipts; U.S. currency exchanges; U.S. wire transfers; safe deposit box lease ☐ Medium risk: ACH originations; frequent purchase of official checks, travelers checks, money orders, or other monetary instruments; frequent access to safe deposit box; frequent currency deposits or withdrawals \$3,000 to \$5,000 ☐ Higher risk: International currency exchanges; international wire transfers; remote deposit capture; or frequent currency deposits or withdrawals over \$5,000
Transactions per month	☐ Lower risk: 1 to 25 ☐ Medium risk: 25 to 50 ☐ Higher risk: 50 or more
Source of opening deposit	☐ Lower risk: Government or payroll check, cash up to \$1,000 ☐ Medium risk: Non-local cashier's check, postal money order, non-local commercial or consumer check, or non-local other government check, or cash \$1,000 to \$5,000 ☐ Higher risk: Wire transfers, travelers checks, private money orders numbered sequentially or with unusual symbols, or cash over \$5,000
Account behavior	Use this space to describe any significant changes in transaction history or behavior
Other	Use this space to describe other risk factors, including accounts and transactions that are not usual and customary for the member or for the credit union

OVERALL RISK RATING:

☐ **Low Risk**
☐ **Moderate Risk**
☐ **High Risk** (requires enhanced due diligence, information collection & monitoring)

Completed by _____ Date _____

Approved by _____ Date _____

© 2011 Wisconsin Credit Union League

EXHIBIT H - CDD RISK MATRIX FOR ORGANIZATIONS

The credit union needs to exercise customer due diligence (CDD) when opening accounts and monitoring existing accounts for suspicious activity. Gather information about account holders at account opening to determine risk, and reassess the risk rating if there is a change in the member's/customer's risk profile (e.g., expected account activity, change in business operations, etc.). Apply enhanced due diligence to monitor activity of high-risk members/customers. Please review The League's ii Release No. 0159 and the FFIEC exam manual for details on CDD. The matrix below is offered only as a guide to help with risk-rating. It must be tailored to the credit union's operations. Because credit unions are each unique, and differ in their size, resources and staff, this matrix will not work for every credit union. Credit unions may consider assigning numerical scores to the various categories.

Account holder's name: _____

Account numbers: _____

Information Needed	Check all that apply
Length of CU membership	☐ Lower risk: 2+ years ☐ Medium risk: 1 to 2 years ☐ Higher risk: Less than 1 year
Age of business	☐ Lower risk: 2+ years ☐ Medium risk: 1 to 2 years ☐ Higher risk: Less than 1 year
Market area	☐ Lower risk: Local ☐ Medium risk: State-wide ☐ Higher risk: National/international
NAICS code <i>www.naics.com</i>	☐ Lower risk: Not listed in high- or moderate-risk NAICS codes ☐ Medium risk: Listed in moderate-risk NAICS codes ☐ Higher risk: Listed in high-risk NAICS codes
Account opening method	☐ Lower risk: In person with all authorized signers ☐ Medium risk: In person with some, but not all, authorized signers ☐ Higher risk: Not opened in person
Geographic location	Consider the primary location of the business and any branches, franchises or other locations; the residences or citizenship of its principals or owners and authorized signers; and the location that is the source of account funds. The follow are higher-risk: ☐ Country subject to OFAC sanctions or otherwise considered higher-risk, such as money laundering centers, supporters of terrorism, offshore financial centers, countries subject to FinCEN advisories, etc. ☐ High-intensity drug trafficking area (including Milwaukee, Waukesha, Racine, Kenosha, Rock, Brown and Dane counties in Wisconsin) <i>www.whitehousedrugpolicy.gov/hidta/</i> ☐ High-intensity financial crimes area (including the Chicago area, New York, New Jersey, southern Florida, northern and southern California, the southwestern U.S. border region, Puerto Rico and the Virgin Islands) <i>www.fincen.gov/law_enforcement/hifca/</i>
Organization type	☐ Lower risk: Corporation; partnership with written agreement; or limited liability company ☐ Medium risk: Sole proprietor; probate estate ☐ Higher risk: Partnership without written agreement; non-profit; lodge or unincorporated association; or organization type that is unusual for credit union
Higher-risk businesses	The following are all higher-risk: ☐ Non-governmental organizations and charities (foreign and domestic) ☐ Non-bank financial institutions (e.g., check cashers, money services businesses) ☐ Casinos and card clubs ☐ Leather goods stores ☐ Car, boat and plane dealerships ☐ Used car or truck dealers and machine parts manufacturers ☐ Travel agencies ☐ Brokers/dealers in securities ☐ Jewel, gem, and precious metal dealers ☐ Auctioneers and pawn brokers ☐ Professional service providers (e.g., attorneys, accountants, doctors and real estate brokers)

Higher-risk businesses (cont'd)	☐ Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages) ☐ Ship, bus, plane operators ☐ Telemarketers ☐ Deposit brokers ☐ Import/export companies ☐ Offshore businesses or banks
CTR/SAR filings	☐ Lower risk: Account holder has no previous CTR or SAR filings ☐ Higher risk: Account holder has previous CTR or SAR filings and should be given an overall risk rating of "high"
Account type	☐ Lower risk: Savings; share certificate ☐ Medium risk: Business checking; revocable living trust; SBA loan ☐ Higher risk: IOLTA; IBRETA; irrevocable trust; commercial loan or line of credit; commercial construction loan
Types of transactions	☐ Lower risk: Occasional currency deposits / withdrawals over \$3,000; internet banking / bill pay; ACH receipts; U.S. currency exchanges; U.S. wire transfers; safe deposit box lease ☐ Medium risk: ACH originations; frequent purchase of official checks, travelers checks, money orders, or other monetary instruments; frequent access to safe deposit box; frequent currency deposits or withdrawals \$3,000 to \$5,000 ☐ Higher risk: International currency exchanges; international wire transfers; remote deposit capture; or frequent currency deposits or withdrawals over \$5,000
Transactions per month	☐ Lower risk: 1 to 25 ☐ Medium risk: 25 to 50 ☐ Higher risk: 50 or more
Source of opening deposit	☐ Lower risk: Government or payroll check, cash up to \$1,000 ☐ Medium risk: Non-local cashier's check, postal money order, non-local commercial or consumer check, or non-local other government check, or cash \$1,000 to \$5,000 ☐ Higher risk: Wire transfers, travelers checks, private money orders numbered sequentially or with unusual symbols, or cash over \$5,000
Account behavior	Use this space to describe any significant changes in transaction history or behavior
Other	Use this space to describe other risk factors, including accounts and transactions that are not usual and customary for the member or for the credit union

_____ **Low Risk**
 _____ **Moderate Risk**
 _____ **High Risk** (requires enhanced due diligence, information collection & monitoring)

Completed by _____ Date _____

Approved by _____ Date _____

© 2011 Wisconsin Credit Union League

EXHIBIT I – FINCEN’S FREQUENTLY ASKED QUESTIONS REGARDING CDD (MAY 2026)

The Financial Crimes Enforcement Network (FinCEN) has issued a consolidated set of *Frequently Asked Questions (FAQs)* regarding customer due diligence requirements for covered financial institutions. For further information regarding customer due diligence requirements, including the CDD Rule, please see FinCEN’s *CDD webpage*.

A. General Questions

A.1. Why did FinCEN issue the CDD Rule?

FinCEN issued the CDD Rule to amend existing Bank Secrecy Act (BSA) regulations in order to clarify and strengthen customer due diligence (CDD) requirements for certain financial institutions. The CDD Rule outlines explicit customer due diligence requirements and imposes a new requirement for these financial institutions to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. Within this construct, as stated in the preamble to the rule, FinCEN intends that the legal entity customer identify its ultimate beneficial owner or owners and not “nominees” or “straw men.”

[Issued July 19, 2016; updated May 6, 2026]

A.2. Does the CDD Rule apply to all financial institutions? No. The CDD Rule applies to covered financial institutions.

No. The CDD Rule applies to covered financial institutions.

[Issued July 19, 2016]

A.3. What was the effective date of the CDD Rule?

July 11, 2016, which was 60 days from the publication of the CDD Rule in the Federal Register.

[Issued July 19, 2016; updated May 6, 2026]

A.4. When must covered financial institutions implement the final rule?

Covered financial institutions had until May 11, 2018, two years from the date the final CDD Rule was published in the Federal Register, to implement and comply with the CDD Rule.

[Issued July 19, 2016; updated May 6, 2026]

A.5. Which financial institutions are covered under the CDD Rule?

For purposes of the CDD Rule, covered financial institutions are federally regulated banks and federally insured credit unions, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities. The term covered financial institution is defined at 31 CFR 1010.605(e)(1).

[Issued July 19, 2016]

A.6. Are there any changes to the AML program requirements for covered financial institutions in the Rule?

Yes. The CDD Rule amends the AML program requirements for each covered financial institution to explicitly require covered institutions to implement and maintain appropriate risk-based procedures for conducting ongoing customer due diligence, to include:

- Understanding the nature and purpose of the customer relationships; and
- Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

A covered financial institution’s AML program must include, at a minimum: (1) a system of internal controls; (2) independent testing; (3) designation of a compliance officer or individual(s) responsible for day-to-day compliance; (4) training for appropriate personnel; and (5) appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships and to conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, to maintain and update customer information.

[Issued July 19, 2016]

B. Beneficial Ownership Information Collection under the CDD Rule

B.1.a. What are the requirements for covered financial institutions to collect beneficial ownership information under the CDD Rule?

The CDD Rule requires covered financial institutions to establish and maintain written procedures that are reasonably designed to identify and verify the beneficial owners of legal entity customers. These procedures must enable the institution to identify the beneficial owners of each legal entity customer at the time a new account is opened, unless the customer is otherwise excluded, the account is exempted, or the covered financial institution chooses to avail itself of the Account Opening Exemptive Relief Order (see Question B.1.b.). In addition, the procedures must establish risk-based practices for verifying the identity of each beneficial owner identified to the covered financial institution, to the extent reasonable and practicable. The procedures must contain the elements required for verifying the identity of customers that are individuals under applicable customer identification program (CIP) requirements located at 31 CFR 1020.220(a)(2), 31 CFR 1023.220(a)(2), 31 CFR 1024.220, and 31 CFR 1026.220(a)(2).

In short, covered financial institutions are required to obtain, verify, and record the identities of the beneficial owners of legal entity customers.

[Issued July 19, 2016; updated May 6, 2026]

B.1.b. What does the Account Opening Exemptive Relief Order authorize?

On February 13, 2026, FinCEN granted exemptive relief to covered financial institutions from the requirements set forth in 31 CFR 1010.230(b) to identify and verify the identities of beneficial owners of legal entity customers at each new account opening—the *Account Opening Exemptive Relief Order*. Rather than having to identify and verify a legal entity customer's beneficial owners each time that customer opens an account, covered financial institutions may instead limit their identification and verification of the identities of beneficial owners under 31 CFR 1010.230(b) to the following circumstances: (1) when a legal entity customer first opens an account with a covered financial institution; (2) any time thereafter when the covered financial institution has knowledge of facts that would reasonably call into question the reliability of beneficial ownership information previously obtained about the legal entity customer; and (3) as needed based on a covered financial institution's risk-based procedures for conducting ongoing customer due diligence.

Whether a covered financial institution chooses to avail itself of the Account Opening Exemptive Relief Order is within the discretion of the covered financial institution. Thus, a covered financial institution may elect to either establish or continue existing customer due diligence processes of identifying and verifying the identities of a legal entity customer's beneficial owners at each new account opening.

[Issued May 6, 2026]

B.2. Must a covered financial institution's procedures for identifying and verifying the identity of beneficial owners of legal entity customers under the CDD Rule be identical to its customer identification program?

No. However, the CDD Rule requires that the procedures, at a minimum, contain the same elements as required for verifying the identity of customers that are individuals under the applicable CIP rule. Additionally, financial institutions may use photocopies or other reproductions of identification documents in the case of documentary verification.

[Issued July 19, 2016]

B.3. Are covered financial institutions required to include the procedures for identifying and verifying the identity of the beneficial owners of legal entity customers in the institution's anti-money laundering (AML) compliance program?

Yes. The CDD procedures must be included in the covered financial institution's AML compliance program.

[Issued July 19, 2016]

B.4. Are covered financial institutions required to collect any information about beneficial ownership from the legal entity customer?

Yes. Covered financial institutions must collect information on individuals who are beneficial owners of a legal entity customer in addition to the information they are required to collect on the customer under the CIP requirement.

[Issued July 19, 2016]

B.5. Who is a “beneficial owner” under the CDD Rule?

The CDD Rule defines “beneficial owner” as each of the following:

- Each individual, if any, who, directly or indirectly, owns 25% or more of the equity interests of a legal entity customer (i.e., the ownership prong); and
- A single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or any other individual who regularly performs similar functions (i.e., the control prong). This list of positions is illustrative, not exclusive, as there is significant diversity in how legal entities are structured.

Under this definition, a legal entity will have a total of between one and five beneficial owners (i.e., one person under the control prong and zero to four persons under the ownership prong).

[Issued July 19, 2016]

B.6. Are covered financial institutions required to obtain information directly from the beneficial owners of legal entity customers?

No. The CDD Rule requires financial institutions to obtain information about the beneficial owners of a legal entity from the individual seeking to open a new account at the covered financial institution on behalf of the legal entity customer. This individual could, but would not necessarily, be a beneficial owner.

[Issued July 19, 2016; updated May 6, 2026]

B.7. What types of information are covered institutions required to collect on the beneficial owners of legal entity customers?

As with CIP for individual customers, covered financial institutions must collect from the legal entity customer the name, date of birth, address, and social security number or other government identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity.

[Issued July 19, 2016]

B.8. May a legal entity provide the identification of a nominee owner in response to a financial institution’s request for the identification of a beneficial owner?

No. As stated in the preamble to the CDD Rule, FinCEN intends that the legal entity customer identify its ultimate beneficial owner or owners and not “nominees” or “straw men.” FinCEN reiterates that it is the responsibility of the legal entity customer to identify its ultimate beneficial owners and that the financial institution may rely upon the information provided, unless the institution has reason to question its accuracy.

[Issued July 19, 2016]

B.9. What types of individuals satisfy the definition of a person with “significant responsibility to control, manage, or direct a legal entity customer?”

Under the CDD Rule, a legal entity must provide information on a control person with “significant responsibility to control, manage, or direct the company.” The Rule also provides examples of the types of positions that could qualify, including “[a]n executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer).” FinCEN’s expectation is that the control person identified must be a high-level official in the legal entity, who is responsible for how the organization is run, and who will have access to a range of information concerning the day-to-day operations of the company. The list of positions is illustrative, not exclusive.

[Issued July 19, 2016]

B.10. Must covered financial institutions collect beneficial ownership information on all of the beneficial owners of a legal entity customer?

Covered financial institutions must collect and verify the beneficial ownership information of each person who meets the definition under the ownership prong, and of one person under the control prong. Under the ownership prong, covered financial institutions are required to collect the beneficial ownership information only for each individual who owns directly or indirectly 25% or more of the equity interest of a legal entity and under the control prong, for one individual with significant responsibility to control, manage, or direct the entity. However, the Rule recognizes that there may be instances when no one individual owns 25% or more of the equity interest of the legal entity; in such instances, the financial institution is still required to collect the required information for one individual who controls, manages, or directs the legal entity customer.

[Issued July 19, 2016]

B.11. Can a covered financial institution adopt and implement more stringent written internal policies and procedures for the collection of beneficial ownership information than the obligations set the CDD Rule and set forth in 31 CFR 1010.230?

Yes. Covered financial institutions may choose to implement stricter written internal policies and procedures for the collection and verification of beneficial ownership information than the requirements prescribed by the CDD Rule.

Transparency in beneficial ownership provides highly valuable information that supports law enforcement, tax, regulatory, or counterterrorism investigations. The Rule sets forth the standard for collecting such valuable information at 25% of beneficial ownership. Therefore, covered financial institutions will meet their beneficial ownership obligations by collecting information on individuals, if any, who hold directly or indirectly, 25% or more of the equity interests in and one individual who has managerial control of a legal entity customer. A covered financial institution may choose, however, to collect such information on natural persons who own a lower percentage of the equity interests of a legal entity customer as well as information on more than one individual with managerial control.

[Issued April 3, 2018; updated May 6, 2026]

B.12. Are there circumstances where covered financial institutions should consider collecting beneficial ownership information at a lower equity interest threshold under the AML program rules with regard to certain customers?

There may be circumstances where a financial institution may determine that collection and verification of beneficial ownership information at a lower threshold may be warranted, based on the financial institution's own assessment of its risk relating to its customer.

Transparency in beneficial ownership, however, is only one aspect of a covered financial institution's customer due diligence obligations. A financial institution may reasonably conclude that collecting beneficial ownership information at a lower equity interest than 25% would not help mitigate the specific risk posed by the customer or provide information useful to the financial institution in analyzing the risk. Rather, any additional heightened risk could be mitigated by other reasonable means, such as enhanced monitoring or collecting other information, including expected account activity, in connection with the particular legal entity customer.

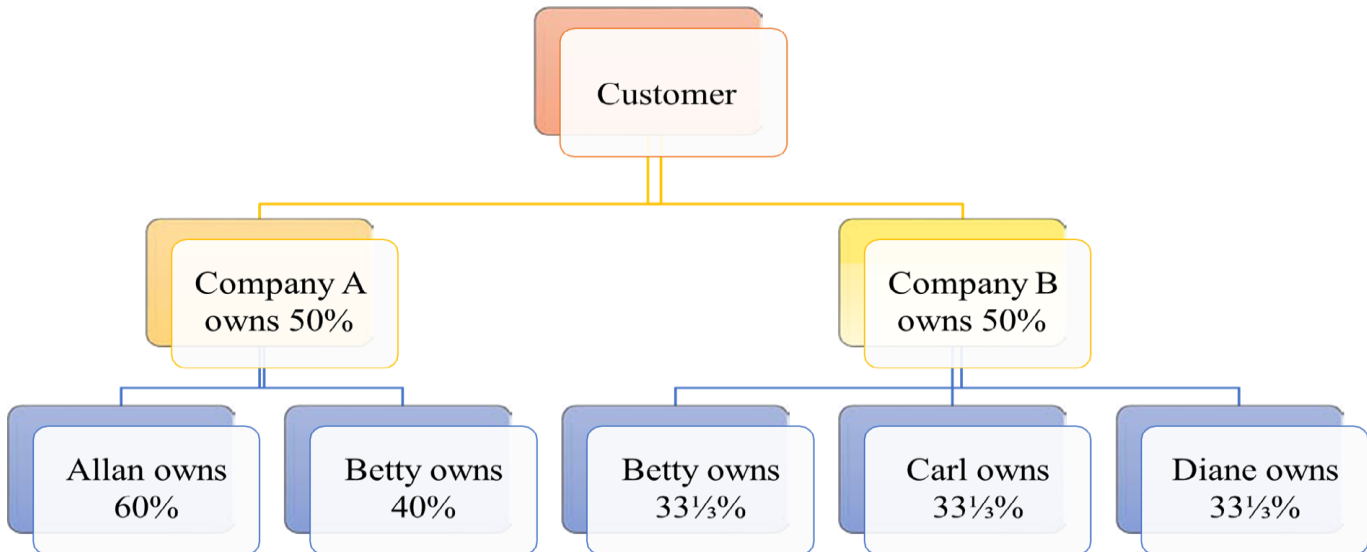
In all cases, however, it is important that covered financial institutions establish and maintain written procedures that are reasonably designed to identify and verify the identity of beneficial owners of legal entity customers and to include such procedures in their AML compliance program.

[Issued April 3, 2018]

B.13. When a legal entity is identified as owning 25% or more of a legal entity customer that is opening an account, is it necessary for a covered financial institution to request beneficial ownership information on the legal entity identified as an owner?

Under the CDD Rule's beneficial ownership identification requirement, a covered institution must collect, from its legal entity customers, information about any individual(s) that are the beneficial owner(s) (unless the entity is excluded or the account is exempted). Therefore, covered financial institutions must obtain from their legal entity customers the identities of individuals who satisfy the definition, either directly or indirectly through multiple corporate structures, as illustrated in the following example.

For purposes of the Rule, Allan is a beneficial owner of Customer because he owns indirectly 30% of its equity interests through his direct ownership of Company A. Betty is also a beneficial owner of Customer because she owns indirectly 20% of its equity interests through her direct ownership of Company A plus 16⅔% through Company B for a total of indirect ownership interest of 36⅔%. Neither Carl nor Diane is a beneficial owner because each owns indirectly only 16⅔% of Customer's equity interests through their direct ownership of Company B.



A covered financial need not independently investigate the legal entity customer's ownership structure and may accept and reasonably rely on the information regarding the status of beneficial owners presented to the financial institution by the legal entity customer's representative, provided that the institution has no knowledge of facts that would reasonably call into question the reliability of the information.

[Issued April 3, 2018]

B.14. What means of identity verification are sufficient to reliably confirm beneficial ownership under the CDD Rule?

Covered financial institutions must verify the identity of each beneficial owner according to risk-based procedures that contain, at a minimum, the same elements financial institutions are required to use to verify the identity of individual customers under applicable CIP requirements. This includes the requirement to address situations in which the financial institution cannot form a reasonable belief that it knows the true identity of the legal entity customer's beneficial owners. Although the CDD Rule's beneficial ownership verification procedures must contain the same elements as existing CIP procedures, they are not required to be identical to them. For example, a covered financial institution's policies and procedures may state that the institution will accept photocopies of a driver's license from the legal entity customer to verify the beneficial owner(s)' identity if the beneficial owner is not present, which is not permissible in the CIP rules. (See Question B.16)

A financial institution's CIP must contain procedures for verifying customer identification, including describing when the institution will use documentary, non-documentary, or a combination of both methods for identity verification. Covered financial institutions may use the same methods to verify the identity of the beneficial owner of a legal entity customer. In addition, in contrast to the CIP rule, the CDD Rule expressly authorizes covered financial institutions to use photocopies or other reproduction documents for documentary verification.

Documentary verification may include unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport. Non-documentary methods of verification may include contacting a beneficial owner; independently verifying the beneficial owner's identity through the comparison of information provided by the legal entity customer (or the beneficial owner, as appropriate) with information obtained from other sources; checking references with other financial institutions; and obtaining a financial statement.

Financial institutions should conduct their own risk-based analysis to determine the appropriate method(s) of verification and the appropriate documents or types of photocopies or reproductions to accept in order to comply with the beneficial owner verification requirement.

[Issued April 3, 2018; updated May 6, 2026]

B.15. What address should be obtained for a legal entity customer's beneficial owner(s) to comply with the certification requirement — residential or business?

The address requirements for certification under the CDD Rule are the same as those outlined in the CIP rule. For an individual beneficial owner, covered financial institutions must obtain either a residential or a business street address. If neither is available, acceptable substitutes may include an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business street address of next of kin or of another contact individual.

[Issued April 3, 2018; updated May 6, 2026]

B.16. What process should a covered financial institution use to identify and verify the identity of a beneficial owner of a legal entity customer when the beneficial owner is unavailable to appear in person during the opening of a new account?

A covered financial institution may identify the beneficial owner(s) of a legal entity customer either by obtaining a completed Certification Form (Appendix A to the Rule) or equivalent information from the legal entity customer's representative and may rely on such information, provided that it has no knowledge of facts that would reasonably call into question the reliability of such information. Furthermore, covered financial institutions may verify the identity of a beneficial owner who does not appear in person, through a photocopy or other reproduction of a valid identity document, or by non-documentary means described in response to Question B.14 above.

[Issued April 3, 2018; updated May 6, 2026]

B.17. If an individual named as a beneficial owner of a new legal entity account is an existing customer of the covered financial institution subject to the financial institution's CIP, is a covered financial institution still required to identify and verify the identity of this individual, or may it rely on the CIP identification and verification of the individual that it previously performed?

Pursuant to the CDD Rule, a covered financial institution must identify and verify the identity of the beneficial owner(s) of legal entity customers at the time each new account is opened. However, pursuant to the Account Opening Exemptive Relief Order, a covered financial institution may, but is not required to, limit its identification and verification of the identities of beneficial owners under the CDD Rule to the following scenarios: (1) when a legal entity customer first opens an account with a covered financial institution, (2) any time thereafter when the covered financial institution has knowledge of facts that would reasonably call into question the reliability of beneficial ownership information previously obtained about the legal entity customer, and (3) as needed based on a covered financial institution's risk-based procedures for conducting ongoing customer due diligence.

If the individual identified as the beneficial owner is an existing customer of the financial institution and is subject to the financial institution's CIP, a financial institution may rely on information in its possession to fulfill the identification and verification requirements, provided the existing information is up-to-date, accurate, and the legal entity customer's representative certifies or confirms (verbally or in writing) the accuracy of the pre-existing CIP information.

For example, a representative of X Corp opens a new account for the company at a covered financial institution and identifies John Doe, who has a personal account at the institution, as a 25% equity owner of X Corp. As required under the CIP rule, the institution identified and verified John Doe's identity at the time the personal account was established. In this situation, a covered financial institution may rely on the pre-existing CIP identification and verification information it maintains for John Doe, provided that X Corp's representative certifies or confirms (verbally or in writing) the accuracy of the pre-existing information on John Doe in order to comply with the Rule. The covered financial institution's records of beneficial ownership for the new account could cross-reference the relevant CIP records, and the verification of information would not need to be repeated.

[Issued April 3, 2018; updated May 6, 2026]

B.18. Are covered financial institutions required to obtain or update beneficial ownership information during routine periodic reviews of existing accounts, absent risk-based concerns; that is, are such reviews a trigger for the application of the Rule's beneficial ownership requirements?

No. Covered financial institutions do not have an obligation to solicit or update beneficial ownership information as a matter of course during regular or periodic reviews, absent specific risk-based concerns. Financial institutions are required to develop and implement risk-based procedures for conducting ongoing customer due diligence, including regular monitoring to identify and report suspicious activity and, on a risk basis, to maintain and update customer information. Thus, periodic reviews are not by

themselves a trigger to obtain or update beneficial ownership information. As stated in response to Question B.20, the obligation to obtain or update information is triggered when, in the course of normal monitoring, a financial institution becomes aware of information about a customer or an account, including a possible change of beneficial ownership information, relevant to assessing or reassessing the customer's overall risk profile. Absent such a risk-related trigger or event, collecting or updating of beneficial ownership information is at the discretion of the covered financial institution. Financial institutions may exercise this discretion to collect or update beneficial ownership information on customers as often as they deem appropriate.

[Issued April 3, 2018]

B.19. If an update to beneficial ownership information is required, can the change(s) be made in a covered financial institution's databases without physically obtaining and re-certifying the information?

It depends. A covered financial institution must develop written internal policies, procedures, and internal controls with respect to collecting, maintaining, and updating a legal entity's beneficial ownership information. The CDD Rule requires the covered financial institutions monitor, and on a risk-basis, update the customer information, including the beneficial ownership information, and does not require re-certification when the information is up-to-date and accurate. Covered financial institutions may therefore update their records to reflect a change of information for an existing beneficial owner using the same or similar processes the institution implemented to record account information it obtains from customers in connection with the institution's account opening processes. For example, if the update were only to a change of address for an existing beneficial owner whose identity information has already been collected and verified, then full re-certification would likely not be required. In this circumstance, it may be reasonable for the covered financial institution to communicate verbally with the legal entity customer to confirm the accuracy of the change of address and reflect such information in its databases. If, however, the updated information were a change of beneficial ownership, then the new beneficial owner's identity would need to be collected, certified, and verified.

[Issued April 3, 2018; updated May 6, 2026]

B.20. Does FinCEN distinguish between the requirements for identifying and verifying beneficial owner information at the time of a new account opening and at the time of a triggering event?

No. Whether a covered financial institution identifies and verifies the identity of the beneficial owner at the time a legal entity initially opens a new account or at the time of a triggering event, the fundamental elements of identification and verification are the same. That is, covered financial institutions must identify each beneficial owner by obtaining their name, date of birth, address, and identifying number (such as a social security number or other identifying number permissible under the CIP rule), and verify their identities. However, financial institutions' written policies, procedures, and processes, as well as the sum of information, may differ with respect to the collection of information at the time a legal entity customer opens a new account or at the time an existing account is updated after a triggering event.

The breadth of information collected as the result of a triggering event during the normal course of monitoring to identify and report suspicious activity and to maintain and update customer information should be determined by what information has changed. That is, only the information that has changed must be updated (e.g., changing the address of the beneficial owner). To the extent that the triggering event results in a determination that the beneficial ownership of the legal entity may have changed entirely, the identity of any new beneficial owner(s) must be collected, certified, and verified, consistent with section 1010.230(b).

[Issued April 3, 2018; updated May 6, 2026]

B.21. Are covered financial institutions required to identify and verify the identity of the beneficial owners that own 25% or more of the ownership interests of a pooled investment vehicle whose operators or advisers are not excluded from the definition of legal entity customer?

No. Although the CDD Rule requires covered financial institutions to collect and verify the identity of beneficial owners who own 25% or more of the equity interests of a legal entity customer, in general, institutions are not required to look through a pooled investment vehicle to identify and verify the identity of any individuals who own 25% or more of its equity interests. Because of the way in which ownership of a pooled investment vehicle fluctuates, it would be impractical for covered financial institutions to collect and verify ownership identity for this type of entity. Therefore, there is no requirement that the financial institution should request the customer to look through the pooled investment vehicle to determine and report any individual's equity interest. However, covered financial institutions must collect beneficial ownership information for the pooled investment vehicle under the control prong to comply with the Rule (i.e., an individual with significant responsibility to control, manage, or direct the vehicle; such individuals could be, e.g., a portfolio manager, commodity pool operator, commodity trading advisor, or

general partner of the vehicle). In cases where such manager, operator or advisor is itself an entity, then it would be necessary to identify an individual with responsibility to control, manage or direct the manager, operator, advisor or general partner.

[Issued April 3, 2018; updated May 6, 2026]

B.22. When 25% or more of the equity interests of a legal entity customer are owned by a trust that is overseen by multiple trustees, are covered financial institutions required to identify and verify the identity of all trustees?

No. If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25% or more of the equity interests of a legal entity customer, the beneficial owner under the ownership/equity prong is the trustee. Where there are multiple trustees, financial institutions are expected to collect and verify the identity of, at a minimum, one trustee of a multi-trustee trust who owns 25% or more of the equity interests of a legal entity customer that is not subject to an exclusion. A covered financial institution may choose to identify additional trustees as part of its customer due diligence, based on its risk assessment and the customer risk profile and in accordance with the institution's account opening procedures.

[Issued April 3, 2018; updated May 6, 2026]

B.23. If a legal entity is the trustee (e.g., law firm, bank trust department, etc.) of a trust that owns 25% or more of the equity interests of a legal entity customer, can that entity be identified as a beneficial owner under the ownership/equity prong or does a natural person need to be so identified?

If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise, 25% or more of the equity interests of a legal entity customer, the beneficial owner for purposes of the ownership/equity prong is the trustee, regardless of whether the trustee is a natural person or a legal entity. In circumstances where a natural person does not exist for purposes of the ownership/equity prong, a natural person would not be identified. However, a covered institution should collect identification information on the legal entity trustee as part of its CIP, consistent with the covered institution's risk assessment and the customer risk profile.

In addition to the ownership/equity prong, covered financial institutions are also required to identify and verify a natural person as the beneficial owner of the legal entity customer under the control prong to comply with the Rule.

The ownership/equity and control prongs, although related, are independent requirements. Thus, satisfaction of, or exclusion from, regulatory obligations under one prong does not mean a covered financial institution's obligations under the other prong are also satisfied or excluded.

[Issued April 3, 2018; updated May 6, 2026]

B.24. Are covered financial institutions required to collect or update beneficial ownership information on customers with accounts opened prior to May 11, 2018, the Rule's applicability date?

Financial institutions are not required to conduct retroactive reviews to obtain beneficial ownership information from customers with accounts opened prior to May 11, 2018. The obligation to obtain or update beneficial ownership information on legal entity customers with accounts established before May 11, 2018, is triggered when a financial institution becomes aware of information about the customer during the course of normal monitoring relevant to assessing or reassessing the risk posed by the customer, and such information indicates a possible change of beneficial ownership.

[Issued April 3, 2018; updated May 6, 2026]

C. Account

C.1. How is "account" defined in the CDD Rule?

In order to maintain consistency with CIP, FinCEN added to the CDD Rule the same definition of the term "account" that is in the CIP rules for banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities.

[Issued July 19, 2016]

C.2. What is a "new account" and does opening a new account require identification and verification of a legal entity customer's beneficial owner(s)?

The CDD Rule defines a "new account" as each account opened at a covered financial institution by a legal entity customer on or after the May 11, 2018, applicability date. Pursuant to the CDD Rule, a covered financial institution must identify and verify

the identity of the beneficial owner(s) of legal entity customers at the time each new account is opened unless the customer is otherwise excluded or the account is exempted. However, pursuant to the Account Opening Exemptive Relief Order, a covered financial institution may, but is not required to, limit its identification and verification of the identities of beneficial owners under the CDD Rule to the following scenarios: (1) when a legal entity customer first opens an account with a covered financial institution, (2) any time thereafter when the covered financial institution has knowledge of facts that would reasonably call into question the reliability of beneficial ownership information previously obtained about the legal entity customer, and (3) as needed based on a covered financial institution's risk-based procedures for conducting ongoing customer due diligence. Refer to the *Account Opening Exemptive Relief Order* for further details.

[Issued July 19, 2016; updated May 6, 2026]

C.3. Does a covered financial institution have to obtain beneficial information on existing accounts?

No. The rule does not cover existing accounts that were opened before the applicability date.

[Issued July 19, 2016]

C.4. Are there any type of accounts that are not covered by the CDD Rule?

Yes. Subject to certain limitations, covered financial institutions are also not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens any of the following four categories of accounts:

- Accounts established at the point-of-sale to provide credit products, solely for the purchase of retail goods and/or services at these retailers, up to a limit of \$50,000;
- Accounts established to finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of the postage products;
- Accounts established to finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker; and
- Accounts established to finance the purchase or lease of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

These exemptions will not apply under either of the following two circumstances:

- If the accounts are transaction accounts through which a legal entity customer can make payments to, or receive payments from, third parties; and
- If there is the possibility of a cash refund for accounts opened to finance purchase of postage, insurance premium, or equipment leasing. If there is the possibility of a cash refund, the financial institution must identify and verify the identity of the beneficial owner(s) either at the initial remittance, or at the time such refund occurs.

[Issued July 19, 2016; updated May 6, 2026]

C.5. FinCEN understands that after a covered financial institution (particularly in the securities and futures industries) opens a new account for a legal entity customer and identifies its beneficial ownership, the financial institution may subsequently open one or more additional accounts or subaccounts for that customer—for the institution's own recordkeeping or operational purposes and not at the customer's specific request—so that the customer may, for example invest in particular products or implement particular trading strategies. Would such accounts fall within the definition of "new accounts" for purposes of the beneficial ownership requirement?

The beneficial ownership requirement applies to a "new account," which is defined to mean "each account opened ... by a legal entity customer" [emphasis added]. An account (or subaccount) relating to a legal entity customer will not be considered a "new account" or an "account" for purposes of the CDD Rule when a financial institution creates such an account (or subaccount) for its own administrative or operational purposes and not at the customer's request—such as to accommodate a specific trading strategy—and the financial institution has already collected beneficial ownership information on such legal entity customer. The distinction between such accounts opened by customers and those opened solely by the financial institution is consistent with the Rule's purpose to mitigate the risks related to the obfuscation of beneficial ownership when a legal entity tries to access the financial system through the opening of a new account. This interpretation is limited to accounts (or subaccounts) created solely to accommodate the business of an existing legal entity customer that has previously identified its beneficial ownership. Thus, the following accounts (or subaccounts) would not fall within this interpretation: accounts (or subaccounts) created to accommodate a trading strategy being carried out by a separate legal entity, including a subsidiary of the existing legal entity

customer; and accounts (or subaccounts) through which the customer of a financial institution's existing legal entity customer carries out trading activity directly through the financial institution without intermediation from the existing legal entity customer.

[Issued April 3, 2018; updated May 6, 2026]

C.6. Are financial institutions required to have their legal entity customers certify the beneficial owners for existing customers during the course of a financial product renewal (e.g., a loan renewal or certificate of deposit)?

Consistent with the definition of "account" in the CIP rules and subsequent interagency guidance, each time a loan is renewed or a certificate of deposit is rolled over, the bank establishes another formal banking relationship, and a new account is established. Pursuant to the CDD Rule, covered financial institutions are required to obtain information on the beneficial owners of a legal entity that opens a new account, meaning (in the case of a bank) for each new formal banking relationship established, even if the legal entity is an existing customer.

Under that framework, covered financial institutions must obtain or request confirmation of certified beneficial ownership information of the legal entity customer product and service renewal at the time of the first renewal following that date. At the time of each subsequent renewal, to the extent that the legal entity customer and the financial service or product (e.g., loan or CD) remains the same, the customer certifies or confirms that the beneficial ownership information previously obtained is accurate and up-to-date, and the institution has no knowledge of facts that would reasonably call into question the reliability of the information, the financial institution would not be required to collect the beneficial ownership information again. In the case of a loan renewal or CD rollover, because we understand that these products are not generally treated as new accounts by the industry and the risk of money laundering is very low, if at the time the customer certifies its beneficial ownership information, it also agrees to notify the financial institution of any change in such information, such agreement can be considered the certification or confirmation from the customer and should be documented and maintained as such, so long as the loan or CD is outstanding.

However, pursuant to the Account Opening Exemptive Relief Order, opening a new account for an existing legal entity customer does not, by itself, require a covered financial institution to identify and verify the identity of the legal entity customer's beneficial owner(s). A covered financial institution may instead—but is not required to—limit its identification and verification of the identities of beneficial owners under the CDD Rule to the following scenarios: (1) when a legal entity customer first opens an account with a covered financial institution, (2) any time thereafter when the covered financial institution has knowledge of facts that would reasonably call into question the reliability of beneficial ownership information previously obtained about the legal entity customer, and (3) as needed based on a covered financial institution's risk-based procedures for conducting ongoing customer due diligence. Consequently, covered financial institutions may choose not to obtain or request confirmation of certified beneficial ownership information from a legal entity customers at the time of renewal of a financial product or service, absent knowledge or need as identified in scenarios (2) or (3) from the *Account Opening Exemptive Relief Order* and in Question B.1.b. Refer to the Account Opening Exemptive Relief Order for details.

[Issued April 3, 2018; updated May 6, 2026]

D. Certification Form

D.1. Are covered financial institutions required to use the beneficial ownership Certification Form (Appendix A to the Rule), and if so, how can they obtain a copy of the Form?

No. There is no requirement that covered financial institutions use the Certification Form. Rather, the form is optional and provided for the convenience of covered financial institutions as one possible method to obtain the required beneficial ownership information. Financial institutions may choose to comply with the requirements of the Rule by using another method, such as through the institutions' own forms, or any other means that comply with the substantive requirements of this obligation.

Covered financial institutions should retain the form and not file it with FinCEN. Covered financial institutions may obtain a fillable and non-fillable copy of the optional Certification Form in Appendix A of the CDD Rule at <https://www.fincen.gov/resources/filing-information>.

[Issued April 3, 2018]

D.2. If a covered financial institution has updated the beneficial ownership information on the account(s) of a legal entity customer, and subsequently a new account is opened on behalf of the same legal entity customer, is the institution required to retain all sets of beneficial ownership documentation, thereby retaining up to three sets of information: the original set collected at account opening, the updated set, and a third, a duplicate of the second (updated) set for the new account?

Covered financial institutions are required to retain all beneficial ownership information collected about a legal entity customer for specified periods. Identifying information, including the Certification Form or its equivalent, must be maintained for a period of five years after that account is closed. All verification records must be retained for a period of five years after the record is made.

Therefore, whether a financial institution must retain a set of identification or verification records is dependent upon the date an account is opened and closed, or the date a record is made. For example, if a covered financial institution relies on pre-existing beneficial ownership information in its possession as true and accurate identification information when opening a new account for a legal entity customer, the financial institution should maintain the original records, and any updated information, including a record of any verbal or written confirmation of pre-existing information until five years after the closing of the new account in order to comply with the recordkeeping requirements in the regulation. Covered financial institutions must also retain a description of every document relied on for verification, any non-documentary methods and results of measures undertaken for verification, as well as the resolution of any substantive discrepancies discovered in identifying and verifying the identification information for five years after the record is made.

[Issued April 3, 2018; updated May 6, 2026]

D.3. If a legal entity customer opens multiple accounts at a covered financial institution (whether or not simultaneously), must the financial institution identify and verify the customer's beneficial ownership for each account?

Pursuant to the CDD Rule, covered financial institutions must identify and verify the legal entity customer's beneficial ownership information for each new account opening, regardless of the number of accounts opened or over a specific period of time. However, an institution that has already obtained a Certification Form (or its equivalent) for the beneficial owner(s) of the legal entity customer may rely on that information to fulfill the beneficial ownership requirement for subsequent accounts, provided the customer certifies or confirms (verbally or in writing) that such information is up-to-date and accurate at the time each subsequent account is opened and the financial institution has no knowledge of facts that would reasonably call into question the reliability of such information. The institution would also need to maintain a record of such certification or confirmation, including for both verbal and written confirmations by the customer.

Additionally, pursuant to the Account Opening Exemptive Relief Order, a covered financial institution may limit its identification and verification of identities of the beneficial owner(s) of a legal entity customer to three scenarios: (1) when the legal entity customer first opens an account with a covered financial institution; (2) any time thereafter when the covered financial institution has knowledge of facts that would reasonably call into question the reliability of beneficial ownership information previously obtained about the legal entity customer; and (3) as needed based on a covered financial institution's risk-based procedures for conducting ongoing customer due diligence. Refer to the *Account Opening Exemptive Relief Order* for further details. When scenario (3) arises—that is, when a covered financial institution determines, based on its risk-based procedures for conducting ongoing customer due diligence, that it needs to identify and verify the beneficial owner(s) of a legal entity customer—the covered financial institution may rely on beneficial ownership information previously obtained in accordance with 31 CFR 1010.230(b)(1), provided the customer certifies or confirms (verbally or in writing) that such information is up-to-date and accurate. The covered financial institution must maintain a record of such certification or confirmation, including for both verbal and written confirmations by the customer.

[Issued April 3, 2018; updated May 6, 2026]

E. Legal Entity Customer

E.1. Who is a "legal entity customer"?

The CDD Rule defines a "legal entity customer" as a corporation, limited liability company, other entity created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account. The definition also includes limited partnerships, business trusts that are created by a filing with a state office, and any other entity created in this manner.

A legal entity customer does not include sole proprietorships, unincorporated associations, or natural persons opening accounts on their own behalf.

[Issued July 19, 2016]

E.2. Are there any entities that are excluded from the definition of the legal entity customer and for which a covered financial institution is not required to obtain beneficial ownership information?

Yes. The CDD Rule excludes from the definition of legal entity customer, certain entities that are subject to Federal or State regulation and for which information about their beneficial ownership and management is available from the Federal or State agencies, such as:

- Financial institutions regulated by a Federal functional regulator or a bank regulated by a State bank regulator;
- Certain exempt persons for purposes of the currency transactions reporting obligations:
 - A department or agency of the United States, of any State, or of any political subdivision of a State;
 - Any entity established under the laws of the United States, or any State, or of any political subdivision of any State, or under an interstate compact;
 - Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York, American, or NASDAQ stock exchange;
 - Any entity organized under the laws of the United States or of any State at least 51% of whose common stock or analogous equity interests are held by a listed entity;
- Issuers of securities registered under section 12 of the Securities Exchange Act of 1934 (SEA) or that is required to file reports under 15(d) of that Act;
- An investment company, as defined in section 3 of the Investment Company Act of 1940, registered with the U.S. Securities and Exchange Commission (SEC);
- An SEC-registered investment adviser, as defined in section 202(a)(11) of the Investment Advisers Act of 1940;
- An exchange or clearing agency, as defined in section 3 of the SEA, registered under section 6 or 17A of that Act;
- Any other entity registered with the SEC under the SEA;
- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, defined in section 1a of the Commodity Exchange Act, registered with the Commodity Futures Trading Commission; and
- A public accounting firm registered under section 102 of the Sarbanes-Oxley Act.

Additional regulated entities:

- A bank holding company, as defined in section 2 of the Bank Holding Company Act of 1956 (12 U.S.C. 1841) or savings and loan holding company, as defined in section 10(n) of the Home Owners' Loan Act (12 U.S.C. 1467a(n));
- A pooled investment vehicle operated or advised by a financial institution excluded from the definition of legal entity customer under the CDD Rule;
- An insurance company regulated by a State; and
- A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

Excluded Foreign Entities:

- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
- A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities; and
- Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620.

[Issued July 19, 2016]

E.3. Are trusts included in the definition of legal entity customer?

No. The definition of legal entity customer only includes statutory trusts created by a filing with the Secretary of State or similar office. Otherwise, it does not include trusts. This is because a trust is a contractual arrangement between the person who provides the funds or other assets and specifies the terms (i.e., the grantor/settlor) and the person with control over the assets (i.e., the trustee), for the benefit of those named in the trust deed (i.e., the beneficiaries). Formation of a trust does not generally require any action by the state.

The CDD Rule does not supersede existing obligations and practices regarding trusts generally. The preamble to each of the CIP rules notes that, while financial institutions are not required to look through a trust to its beneficiaries, they “may need to take additional steps to verify the identity of a customer that is not an individual, such as obtaining information about persons with control over the account.” We understand that where trusts are direct customers of financial institutions, financial institutions generally also identify and verify the identity of trustees, because trustees will necessarily be signatories on trust accounts. Furthermore, under supervisory guidance for banks, “in certain circumstances involving revocable trusts, the bank may need to gather information about the settlor, grantor, trustee, or other persons with the authority to direct the trustee, and who thus have authority or control over the account, in order to establish the true identity of the customer.”

[Issued July 19, 2016; updated May 6, 2026]

E.4. Are sole proprietorships formed by spouses or other unincorporated associations considered legal entity customers under the CDD Rule?

No. Sole proprietorships—individual or spousal—and unincorporated associations are not legal entity customers as defined by the Rule, even though such businesses may file with the Secretary of State in order to register a trade name or establish a tax account. This is because neither a sole proprietorship nor an unincorporated association is a separate legal entity from the associated individual(s), and therefore beneficial ownership is not inherently obscured.

[Issued April 3, 2018; updated May 6, 2026]

E.5. What methods should covered financial institutions use to verify eligibility for exclusion from the definition of a “legal entity customer”?

Several types of legal entity customers are excluded from the collection and verification requirements of the Rule, under section 1010.230(e)(2), because, for example, their regulators require the reporting of beneficial ownership information or such information is publicly available. A financial institution may rely on information provided by the legal entity customer to determine whether the legal entity is excluded from the definition of a legal entity customer, provided that it has no knowledge of facts that would reasonably call into question the reliability of such information. Whether a financial institution has such knowledge would depend on the facts and circumstances at the time an account is opened. Covered financial institutions must establish and maintain written risk-based procedures reasonably designed to identify and verify the identity of the beneficial owners of all legal entity customers at the time a new account is opened, unless the customer is otherwise excluded from the definition of legal entity customer. Covered financial institutions are expected to address and specify, in their risk-based written policies and procedures, the type of information they will obtain and reasonably rely upon to determine eligibility for exclusions.

[Issued April 3, 2018]

E.6. Are covered financial institutions limited to the Internal Revenue Code (IRC) definitions of charities, non-profits, or similar entities when assessing their eligibility for exclusion from the definition of legal entity customer?

No. The exclusion from the definition of legal entity customer for charities and non-profit entities is not limited to those entities that meet the definition or description of charitable, nonprofit, or similar entities under the IRC. The Rule does not rely on the tax-exempt status of an entity as described in the IRC. All nonprofit entities—whether or not tax-exempt—that are established as a nonprofit, or nonstock corporation, or similar entity that has been validly organized with the proper State authority are excluded from the ownership/equity prong of the requirement because nonprofit entities generally do not have ownership interests. Financial institutions, however, are required to collect beneficial ownership information under the control prong from any such entity.

[Issued April 3, 2018; updated May 6, 2026]

E.7. Are companies publicly traded in the United States and entities listed on foreign exchanges excluded from the definition of legal entity customer and, therefore, excluded by the Rule?

Companies traded publicly in the United States are excluded from the definition of legal entity customer. Specifically, the Rule excludes from the definition of legal entity customer certain entities that are considered “exempt persons” under 31 CFR 1020.315(b). This includes any company (other than a bank) whose common stock or analogous equity interests are listed on the New York Stock Exchange, the American Stock Exchange (currently known as NYSE American), or NASDAQ stock exchange. The Rule also excludes a U.S. entity when at least 51% of its common stock or analogous equity interest is held by a listed entity. These U.S. companies are excluded from the Rule because they are subject to public disclosure and reporting requirements that provide information similar to what would otherwise be collected under the Rule.

Companies listed on foreign exchanges are not excluded from the definition of legal entity customer. Such companies may not be subject to the same or similar public disclosure and reporting requirements as companies publicly traded in the United States and, therefore, collecting beneficial ownership information for them is required.

[Issued April 3, 2018; updated May 6, 2026]

E.8. May covered financial institutions take a risk-based approach for collecting beneficial ownership information from legal entity customers listed on foreign exchanges?

No. Financial institutions may not take a “risk-based approach” to collecting the required beneficial ownership information from legal entity customers that are listed on foreign exchanges, because such institutions are not excluded from the definition of legal entity customer. However, as they may with regard to other legal entity customers, whether listed or not, covered institutions may rely on the public disclosures of such entities, absent any reason to believe such information is inaccurate or not up-to-date.

[Issued April 3, 2018]

E.9. Does the exclusion for foreign financial institutions from the Rule’s definition of “legal entity customer” depend on whether the beneficial ownership requirements applied by such institution’s foreign regulator match U.S. requirements?

No. For purposes of beneficial ownership identification, the CDD Rule excludes from the definition of “legal entity customer” a foreign financial institution created in a non-U.S. jurisdiction when the foreign regulator for that financial institution collects and maintains information on the beneficial owner(s) of the regulated institution. The CDD Rule does not require covered financial institutions to research the specific transparency requirements imposed on a foreign financial institution by its regulator and compare them with those imposed on U.S. financial institutions by U.S. Federal functional regulators. However, if the foreign regulator does not collect and maintain beneficial ownership information on the foreign financial institution it regulates, then U.S. financial institutions will have to collect and maintain beneficial ownership information on accounts opened by foreign financial institutions in compliance with the CDD Rule. As with any exclusion, covered financial institutions may rely on the representations of its legal entity customer as to whether an exclusion applies, provided that they have no knowledge of facts that would reasonably call into question the reliability of such representation. (See Question E.5.)

For purposes of existing customer due diligence requirements, covered financial institutions that maintain correspondent accounts for foreign financial institutions are already required to establish and maintain specific risk-based due diligence procedures and controls for such accounts that include consideration of all relevant factors, and are required to identify beneficial ownership for certain high-risk foreign banks. These correspondent accounts will continue to be subject to these existing requirements rather than the requirements set forth in the AML Program requirements contained in the CDD Rule.

[Issued April 3, 2018; updated May 6, 2026]

E.10. Will the U.S. Government maintain a list of non-U.S. jurisdictions where the regulator of financial institutions within that jurisdiction maintains beneficial ownership information regarding the financial institutions they regulate or supervise?

No. Covered financial institutions should contact the relevant foreign regulator or use other reliable means to ascertain whether the foreign regulator maintains beneficial ownership information for the financial institutions that it regulates or supervises.

[Issued April 3, 2018]

E.11. What types of entities would be considered a “non-U.S. governmental department, agency, or political subdivision that engages only in governmental rather than commercial activities” such that they would qualify for exclusion from the definition of a legal entity customer?

Examples of legal entity customers that would be considered non-U.S. governmental entities engaged in only governmental and not commercial activities include entities that are owned and operated by a non-U.S. government agency or political subdivision, such as embassies or consulates, as well as entities that are instrumentalities of a foreign government, such as government-owned enterprises engaging in activities that are exclusively governmental in nature, that is, activities involving the direct exercise of legislative, executive, or judicial authority and which do not involve taking profits from the endeavor. Those State-owned enterprises engaged in profit-seeking activities, including, among others, sovereign wealth funds, airlines, or oil companies, would not qualify for the legal entity customer exclusion. Generally, many State-owned enterprises may not have an individual that owns at least a 25% equity interest because a governmental department, agency, or political subdivision holds such interest.

In these circumstances, a covered financial institution would only be required to identify an individual under the control prong. Similarly, with respect to a State-owned enterprise that is a pooled investment vehicle not subject to another exclusion, financial institutions would be required to obtain beneficial ownership information under the control prong but not under the ownership/equity prong of the definition of beneficial owner.

Furthermore, similar to other instances of identification and verification within the Rule's context, a covered financial institution may reasonably rely upon the representations of the legal entity customer, absent knowledge of facts that would call into question the reliability of the beneficial ownership information provided to the financial institution.

[Issued April 3, 2018; updated May 6, 2026]

E.12. Does the point of sale exception only apply to accounts opened at the cash register or does it refer to all applications for credit accounts that are for use at the private label retailer only?

The CDD Rule provides an exemption from the requirements for a covered financial institution that “opens an account for a legal entity customer that is: [a]t the point-of-sale to provide credit products, including commercial private label credit cards, solely for the purchase of retail goods and/or services at these retailers, up to a limit of \$50,000.” The point of sale exemption is provided for retail credit accounts opened to facilitate purchases made at the retailer because of the very low risk posed by opening such accounts at the brick and mortar store.

[Issued April 3, 2018]

E.13. What kind of businesses and equipment are covered under the equipment finance exemption?

The CDD Rule reflects FinCEN's understanding that businesses require financing to obtain equipment to conduct ongoing business operations. Many such businesses, including both large and small businesses, open accounts solely for the purpose of financing the purchase or lease of that equipment. Subject to certain limitations, the CDD Rule provides an exemption from the requirement to identify and verify the identity of a legal entity customer's beneficial owners for equipment finance and lease accounts established at a covered financial institution because of the low risk for money laundering posed by these accounts. The exemption is intended to cover business equipment such as farm equipment, construction machinery, aircraft, computers, printers, photocopiers, and automobiles that a business purchases or leases. The Rule does not limit the exemption to small businesses. Regardless of the application of the exemption, a covered financial must comply with all other applicable BSA/AML obligations, which may include the obligation to file SARs where there is a suspicion that the equipment may be used to facilitate criminal activity.

[Issued April 3, 2018; updated May 6, 2026]

E.14. Does the equipment lease and purchase exemption apply when the customer leases directly from the covered institution?

Yes, consider the following. Aviation LLC, which operates several flight training schools, visits Aircraft Vendor to acquire five aircraft for its flight training schools. Aviation LLC selects the aircraft and contacts the Lessor Covered Financial Institution to obtain the necessary equipment finance to acquire the aircraft. After a review of the aircraft and Aviation LLC's business, the Lessor Covered Financial Institution agrees to purchase the aircraft from Aircraft Vendor and then lease them to Aviation LLC for a specified rent amount and duration. The Lessor Covered Financial Institution purchases the aircraft, pays the purchase price directly to Aircraft Vendor, and obtains title to the aircraft as collateral. The Lessor Covered Financial Institution then enters into a lease agreement with Aviation LLC, which opens an account at the financial institution solely for the purpose of obtaining the aircraft and making periodic rent payments. There is no possibility of a cash refund to Aviation LLC under the lease terms.

The equipment lease and purchase exemption would apply because the account established at the covered financial institution meets all of the requirements of the exemption, which are that: (1) the account's purpose is to finance the purchase or leasing of equipment; (2) payments are remitted directly by the financial institution to the vendor or lessor; and (3) there is no possibility of a cash refund on the account activity. First, Covered Financial Institution remit full payment directly to the vendor and obtained title to the equipment in order to lease the equipment to the legal entity customer. Second, Aviation LLC opened the account solely for the purpose of financing an equipment lease to acquire aircraft for its training schools. Finally, there is no possibility of a cash refund to Aviation LLC. As noted in the final rule, accounts created to provide financing for equipment lease or purchase, subject to certain conditions, are exempt from the beneficial ownership requirement because they present a low risk for money laundering and terrorist financing.

[Issued April 3, 2018; updated May 6, 2026]

F. Nature and Purpose/Customer Risk Profile/Ongoing Monitoring

F.1. The CDD Rule requires financial institutions to understand “the nature and purpose of customer relationships to develop a customer risk profile.” What type of information should financial institutions collect to satisfy this requirement and may the documentation of the nature and purpose of a customer relationship be made on a risk-basis?

Understanding the nature and purpose of a customer relationship in order to develop a customer risk profile is an important part of ongoing customer due diligence, and is required for all customers and accounts. An understanding based on category of customer means that for certain lower-risk customers, a financial institution's understanding of the nature and purpose of a customer relationship can be developed by inherent or self-evident information, such as the type of customer or type of account, service, or product or other basic information about the customer, including information obtained at first account opening.

The profile may, but need not, include a system of risk ratings or categories of customers. Accordingly, the documentation that is required to demonstrate an understanding of the nature and purpose of a customer relationship would vary with the type of customer, account, service, or product.

[Issued April 3, 2018]

F.2. Once the nature and purpose of a customer relationship has been established, what are FinCEN's expectations concerning the use of this information?

Understanding the nature and purpose of a customer relationship—the information gathered about a customer at account opening—is essential to developing a customer risk profile. This information should be used to develop a baseline against which customer activity, such as the customer's expected use of wires or typical number of deposits in a month, can be assessed for possible suspicious activity reporting. If account activity changes, particularly with regard to what should be anticipated based on the original nature and purpose of the account, risk-based monitoring may identify a need to update customer information, including, as appropriate, beneficial ownership.

[Issued April 3, 2018]

F.3. In understanding the nature and purpose of customer relationships, are financial institutions required to develop and document customer risk profiles for self-evident products or customer type (e.g., a safe deposit box)?

Financial institutions must implement risk-based procedures as part of their AML program to demonstrate an understanding of the nature and purpose of customer relationships to develop customer risk profiles. Customer risk profiles refer “to the information gathered about a customer at account opening used to develop a baseline against which customer activity can be assessed for suspicious activity reporting. This may include self-evident information such as the type of customer, or type of account, service or product.” It is reasonable that in the case of certain products, such as safety deposit boxes, the nature and purpose are self-evident and therefore no additional documentation would be needed to demonstrate an understanding of their nature and purpose, beyond the documentation to establish the particular type of account.

[Issued April 3, 2018; updated May 6, 2026]

F.4. Is it a requirement under the CDD Rule that covered financial institutions:

- **Collect information about expected activity on all customers at account opening, or on an ongoing or periodic basis;**

- **Conduct media searches or screening for news articles on all customers or other related parties, such as beneficial owners, either at account opening, or on an ongoing or periodic basis; or**
- **Collect information that identifies underlying transacting parties when a financial institution offers correspondent banking or omnibus accounts to other financial institutions (i.e., a customer's customer)?**

The CDD Rule does not categorically require: (1) the collection of any particular customer due diligence information (other than that required to develop a customer risk profile, conduct monitoring, and collect beneficial ownership information); (2) the performance of media searches or particular screenings; or (3) the collection of customer information from a financial institution's clients when the financial institution is a customer of a covered financial institution.

A covered financial institution may assess, on the basis of risk, that a customer's risk profile is low, and that, accordingly, additional information is not necessary for the covered financial institution to develop its understanding of the nature and purpose of the customer relationship. In other circumstances, the covered financial institution might assess, on the basis of risk, that a customer presents a higher risk profile and, accordingly, collect more information to better understand the customer relationship.

Covered financial institutions must establish policies, procedures, and processes for determining whether and when, on the basis of risk, to update customer information to ensure that customer information is current and accurate. Information collected throughout the relationship is critical in understanding the customer's transactions in order to assist the financial institution in determining when transactions are potentially suspicious.

[Issued August 3, 2020]

F.5. Is it a requirement under the CDD Rule that covered financial institutions:

- **Use a specific method or categorization to risk rate customers; or**
- **Automatically categorize as "high risk" products and customer types that are identified in government publications as having characteristics that could potentially expose the institution to risks?**

It is not a requirement that covered financial institutions use a specific method or categorization to establish a customer risk profile. Further, covered financial institutions are not required or expected to automatically categorize as "high risk" products or customer types listed in government publications.

Various government publications provide information and discussions on certain products, services, customers, and geographic locations that present unique challenges and exposures regarding illicit financial activity risks. However, even within the same risk category, a spectrum of risks may be identifiable and due diligence measures may vary on a case-by-case basis.

A covered financial institution should have an understanding of the money laundering, terrorist financing, and other financial crime risks of its customers to develop the customer risk profile. Furthermore, the financial institution's program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the risks of its customers. There are no prescribed risk profile categories, and the number and detail of these categories can vary.

[Issued August 3, 2020]

F.6. Is it a requirement under the CDD Rule that financial institutions update customer information on a specific schedule?

There is no categorical requirement that financial institutions update customer information on a continuous or periodic schedule. The requirement to update customer information is risk based and occurs as a result of normal monitoring. Should the financial institution become aware as a result of its ongoing monitoring of a change in customer information (including beneficial ownership information) that is relevant to assessing the risk posed by the customer, the financial institution must update the customer information accordingly. Additionally, if this customer information is relevant to assessing the risk of a customer relationship, then the financial institution should reassess the customer risk profile/rating and follow established financial institutions policies, procedures, and processes for maintaining or changing the customer risk profile/rating. However, financial institutions, on the basis of risk, may choose to review customer information on a regular or periodic basis.

[Issued August 3, 2020]

F.7. Are covered financial institutions required to implement different processes than currently established to comply with the Rule's ongoing monitoring and updating requirement?

To the extent that a covered financial institution has monitoring processes in place that allow the institution to meet the Rule's requirements, such institution may use its existing monitoring processes to comply with customer due diligence monitoring and updating obligations. As the preamble to the Rule states, "current industry practice to comply with existing expectations for SAR reporting should already satisfy this proposed requirement."

[Issued April 3, 2018; updated May 6, 2026]

G. Other

G.1. Are covered financial institutions required to comply with the OFAC regulations with respect to beneficial ownership information?

Covered financial institutions should use beneficial ownership information as they use other information they gather regarding customers (e.g., through compliance with the CIP requirements), including for compliance with OFAC-administered sanctions.

[Issued July 19, 2016]

G.2. Do covered financial institutions now have additional obligations under section 314(a) for beneficial ownership information?

FinCEN does not expect the information obtained under the CDD Rule to add additional 314(a) requirements for financial institutions. The regulation implementing section 314(a) does not require the reporting of beneficial ownership information associated with an account or transaction matching a named subject in a 314(a) request. Covered financial institutions are required to search their records for accounts or transactions matching a named subject and report whether a match exists using the identifying information provided in the request.

[Issued July 19, 2016]

G.3. Under what circumstances should the transactions of a legal entity customer and those of the beneficial owner(s) be aggregated for purposes of filing a CTR? Are financial institutions required to proactively cross-check beneficial ownership information to comply with the CTR aggregation requirement?

As a general matter, financial institutions are required to aggregate multiple currency transactions "if the financial institution has knowledge that [the multiple transactions] are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 during any one business day." With respect to legal entity customers that may share a common owner, unless there is an affirmative reason to believe otherwise, covered financial institutions should presume that different businesses that share a common owner are operating separately and independently from each other and from the common owner. Thus, absent indications that the businesses are not operating independently (e.g., the businesses are staffed by the same employees and are located at the same address, the accounts of one business are repeatedly used to pay the expenses of another business or of the common owner), financial institutions should not aggregate transactions involving those businesses with those of each other or with those of the common owner for CTR filing.

[Issued April 3, 2018; updated May 6, 2026]

G.4. When completing a CTR for a business (i.e., corporations, limited liability companies, and general partnerships) will beneficial owners now need to be listed as beneficiaries in such CTRs? If yes, would this also include trust and estate accounts?

No. The CDD Rule does not change the existing currency transaction reporting requirements or any guidance FinCEN published pursuant to this reporting requirement. Thus, a covered financial institution is not required to list the beneficial owners of a business, or trust or estate account, when completing a CTR as a matter of course. A financial institution must list a beneficial owner in Part 1 of the CTR only if the financial institution has knowledge that the transaction(s) requiring the filing is made on behalf of the beneficial owner and results in either cash in or cash out totaling more than \$10,000 during any one business day.

[Issued April 3, 2018]

G.5. Are covered financial institutions now required to follow specific procedures to approve changes to AML programs or require Boards of Directors or senior management to approve such changes? Can Federal functional regulators direct financial institutions within their jurisdiction to follow a specific approval process?

Covered financial institutions may continue to follow their existing internal procedures for approving AML program changes, including changes that incorporate the Rule's new program requirements. However, these procedures should be consistent with the requirements and expectations of the institution's Federal functional regulator.

[Issued April 3, 2018]