ABA course content is not a substitute for professional legal advice.
Menu

Introduction
Customers and Accounts Under CIP
CIP: Two-Step Process
Recordkeeping Requirements
Reliance on Other Parties
Customer Identification and Account Opening
Wrap Up
Introduction

This course describes the two-step process to obtain types of identifying information from customers, and risk-based procedures to verify information. It explains the procedures to maintain records of the information used to verify identifying information. This course explores different ways to disclose the Customer Information Program (CIP) notice at account opening.

Version: 2.0

Update: July 2019. Added information on Section 213 of S2155 regarding use of photocopies of ID for online account opening.

ABA course content is not a substitute for professional legal advice.

Page 1
Introduction

Overview
Following the September 11, 2001 terrorist attacks, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, (USA PATRIOT Act). The USA PATRIOT Act includes measures to weaken terrorist financing and combat money laundering, and part of this effort involves customer identification programs for persons establishing new accounts. Financial institutions were required by §326 of the PATRIOT Act to establish Customer Identification Programs (CIP).

The CIP rule requires banks and other financial institutions to adopt written procedures to ensure proper identification of new customers. The requirements go beyond just verifying a customer’s identity. Banks must now keep records of identifying information and check customer names against terrorist lists. This applies to any financial institution that opens a new account.

The USA PATRIOT Act requires CIPs for a broad category of companies that fall under the definition of “financial institution,” a term defined by the Bank Secrecy Act. The list includes the following institutions:

- Commercial banks (including foreign banks operating in the United States)
- Credit unions
- Trust and investment companies
- Securities brokers and dealers
- Insurance companies
- Travel agents
- Pawnbrokers
- Dealers in precious metals
- Money services businesses (MSBs)
- Casinos

The USA PATRIOT Act requires CIPs for a broad category of companies that fall under the definition of “financial institution,” a term defined by the Bank Secrecy Act. The list includes the following institutions:
Introduction

Each bank’s CIP must include account-opening procedures that specify the identifying information that the bank will obtain from each customer. The bank must base its procedures on a risk assessment conducted by each bank’s BSA officer and upper level management. The bank should base its risk assessment on the following considerations:

**The types of accounts offered by the bank.** Does the bank primarily offer individual checking and savings accounts, or does it offer more commercial or private banking accounts? The more complicated the account, the greater the risk for the bank.

**The bank’s methods of opening accounts.** Does the bank only open accounts face-to-face, or can customers open accounts or apply for loans online or by telephone? Accounts that are opened remotely pose a greater risk to the bank.

**The types of identifying information available.** Do most of the bank’s customers have state-issued driver’s licenses or are a large percentage of its customers immigrants?

**The bank’s size, location, and customer base, including types of products and services used by customers in different geographic locations.** Does the bank’s customer base consist of mostly foreign individuals? Are they highly transient or longtime residents? Is the bank a large international bank, or a small community bank? Does the bank offer brokerage service or insurance services? The larger the bank and the more diversified the customer base and the products offered, the higher the risk is for the bank.
Introduction

Objectives
By the end of *BSA/AML: CIP Basics*, you will be able to:

- Identify what constitutes an account and a customer under the Customer Information Program (CIP) rule
- Examine the actions to be taken in the two-step process of obtaining identifying information and verifying the identity of the customer
- Identify the procedures for maintaining records of the information used to verify a person's identifying information
- Adhere to established controls and review procedures for reliance on other parties
- Identify methods for handling the CIP notice at account opening
Customers and Accounts Under CIP

All banks must have a written, board approved, Customer Identification Program (CIP). The program must be part of the bank’s Bank Secrecy Act policy and each affected employee must receive training.

Who is a customer?
The CIP rule applies to any person who opens a new account. Under CIP, a “person” is defined as an individual, a corporation, partnership, a trust, an estate, or any other legal entity. A customer is also an individual who opens a new account for another individual who lacks legal capacity, such as a minor, or an individual who opens a new account for an entity that is not a legal person, such as a civic club.

Examples
- If an individual opens a checking account, the bank must identify that person.
- If an individual opens a corporate account, the corporation is the person that the bank must identify. (Some banks also, by policy, require that the person opening the account on behalf of the corporation be identified as well, but this is not required by law unless the entity is defined by the bank as high risk entity such as a money services business. However, see the Frontline Course: BSA-AML: Beneficial Ownership and CDD regarding identification of beneficial owners of legal entity customers.)
- If an individual opens an account as custodian for a minor, the custodian is the person who the bank must identify.
- If a person with power of attorney opens an account for another person or entity, the bank should identify both individuals.
- If a person purchases a general-purpose prepaid card that allows the customer the ability to reload funds, or provides access to credit or overdraft features, the person is a customer for CIP purposes.

Note: For additional information about establishing accounts for entities and about CIP procedures involving prepaid cards, refer to the ABA Frontline Compliance course, BSA/AML: CIP Advanced.
Customers and Accounts Under CIP

Beneficial owners
On May 11, 2016, the Financial Crimes Enforcement Network (FinCEN) published a rule on Customer Due Diligence Requirements for Financial Institutions. The mandatory effective date for compliance with the rule was May 11, 2018. Under the rule, banks are required to collect information of the beneficial owners of legal entity customers and then verify the identity of those individuals using standard Customer Identification Program (CIP) procedures. Customers will be required to provide information on the identity of the individual who has authority to control the entity and any individuals who hold an equity interest in the entity of 25% or more.

The Beneficial Ownership Rule requires banks to establish and maintain written procedures, reasonably designed to identify and verify the beneficial owners of legal entity customers. These procedures must enable the bank to identify the beneficial owners of each customer at the time the bank opens a new account, unless the law excludes the customer or the account is exempt. Also, the procedures must establish risk-based practices for verifying the identity of each beneficial owner identified to the bank, to the extent that is reasonable and practicable. The procedures must contain the elements required for verifying the identity of customers that are individuals under applicable CIP requirements, except that the beneficial ownership rule allows banks to use copies of identification documents. In short, covered financial institutions are now required to obtain, verify, and record the identities of the beneficial owners of legal entity customers.

For an in-depth look at beneficial ownership, see the Frontline Course: BSA-AML: Beneficial Ownership and CDD.
Customers and Accounts Under CIP

What is an account?
Under the CIP rules, a person’s status as a customer equates with account holders. An account is a formal banking relationship that provides services or other financial transactions, such as deposit accounts, loans, credit cards, a safe deposit box, or other safekeeping services or cash management, custodian, or trust services.

A reloadable prepaid card is an account when purchased or when the reload or overdraft feature is activated by cardholder registration. Non-reloadable prepaid cards such as government benefit or payroll cards that cannot be reloaded from other sources are not accounts for BSA purposes.

A consumer or business that is not an account holder at your bank but uses your bank’s services to cash a check drawn on your bank, purchase a money order, or send a wire, does not establish a formal relationship with the bank. Because there is no formal account relationship, that person or entity is not a customer for CIP purposes.

Note: Other BSA recordkeeping requirements such as currency transaction reporting and suspicious activity reporting apply to all banking activity taking place at or through your bank regardless of whether a customer is involved or not.
Customers and Accounts Under CIP

» Roll over the categories below to see the accounts and products that are and are not applicable to CIP.

Insurance products
CIP applies to any insurance product or relationship established to provide ongoing services or financial transactions. The law applies to any product that contains a “retained value” feature, also known as a cash value or investment feature. This includes, but is not limited to the following products:

- Whole Life
- Universal Life
- Single Premium Life
- Annuities

Due to the product structure, the following products are not conducive to money laundering and/or terrorist financing. Therefore, the bank need not establish a CIP program for the following products:

- Consumer Property and Casualty Insurance products or services
- Commercial Property and Casualty products
- Bonding, including Surety Bonds

Traditional bank products
An account includes, but is not limited to, the following transactions and services:

- Traditional types of accounts such as a checking, savings, and certificates of deposit
- Loans and other extensions of credit
- Relationships established to provide safe deposit box and other safekeeping services
- Cash management
- Custodial and trust services
- IRAs/SEPs
- Trusts and investment management
- Financial planning and advisory services
- Some prepaid cards (reloadable)

The law does not apply to the following banking transactions and services:
BSA/AML: CIP Basics

- Products or services where a formal banking relationship has not been established, such as the occasional purchase of Official Checks or Traveler’s Checks
- ATM use
- Cashing checks for noncustomers
- Accounts established for the purpose of participating in an employee benefit plan funded through payroll deductions
- Accounts acquired through merger or acquisition. (However, due diligence should ensure the existence of an established CIP program that met the regulatory requirements)

**Note:** Prepaid Cards: In March 2016, the federal financial regulators, along with the Financial Crimes Enforcement Network, issued guidance to depository institutions on how to apply customer identification programs to the prepaid cards they issue: [https://www.fincen.gov/statutes_regs/guidance/pdf/InterAgencyGuidance20160318.pdf](https://www.fincen.gov/statutes_regs/guidance/pdf/InterAgencyGuidance20160318.pdf). While the guidance does not change or add to existing expectations, it clarifies that banks should apply their CIPs to the cardholders of prepaid cards that constitute “accounts.”

Prepaid cards qualify as accounts if they are reloadable or if they include access to credit or overdraft features. For example, general purpose prepaid cards that are sold without these features activated would not count for CIP purposes until the cardholder activates such a function.

To verify the identity of the account holder as required by the CIP rule, banks must identify the cardholder of a prepaid card that meets the above requirements, even if a third party is the named account holder; third parties are to be treated as agents of the bank rather than customers for CIP purposes. However, if a third-party prepaid card such as a payroll, government benefit or health savings account card does not offer reloading or credit features, the third-party provider would be considered the customer for CIP purposes.
Customers and Accounts Under CIP

Self Check Quiz

Which three individuals would be considered customers for CIP purposes?

» Select the correct answers and click Submit.

A) Mrs. Jones, who opens a trust account for her nephew
B) Mr. Smith, who is added to his wife’s account as a joint signer
C) Ms. Mitchell, who opens a safe deposit box but has no other bank relationship
D) Mr. Rowe, who cashes his payroll check at your branch but has no other bank relationship

A, B, and C are correct.
D is incorrect because Mr. Rowe has not established an ongoing customer relationship with the bank.
The CIP should enable the bank to form a reasonable belief that it knows the true identity of each customer. Even though a CIP is expected to be risk-based, and therefore tailored to each bank's operations, each bank's CIP must contain account-opening procedures that require the bank to obtain certain minimum types of identifying information from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer.

Fundamentally, CIP is a two-step process where the first step is obtaining identifying information and the second step is verifying that the information provided identifies the customer.
CIP: Two-Step Process

Step one
The first step of a CIP is to obtain customer information. This step must include the collection of the customer’s name, street address, birth date (except for an entity), and a government-issued identification number. The customer’s name, street address, and date of birth (individuals) are required pieces of information that a bank must obtain from ALL customers opening a new account. What qualifies as an acceptable government identification number differs depending on whether your customer is a U.S. person or a non-U.S. person.

At a minimum, the bank must obtain the following identifying information from each customer before opening an account.

» Roll over the types of information below to see the descriptions.

Name

Street address

Government-issued identification number

Date of birth

Note
If an individual or business attempts to open an account without the required information discussed above, the bank should not open the account or book the loan until the bank obtains that information.

At a minimum, the bank must obtain the following identifying information from each customer before opening an account.

U.S. citizen or a non-U.S. citizen

Name
Must be the person’s legal name. For example, if the customer’s name is Thaddeus Bartholomew Wentworth, III, but everyone calls him Tad, you still must use Thaddeus Bartholomew Wentworth. Use of suffixes such as Jr., Sr., III, etc., is not required unless the customer wants that information included. In fact, if someone is a “Jr” and his father dies, the Jr is usually dropped.

Street address
- For an individual, this must be a residential street address
- For active duty military and their dependents, 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

Note: A bank should require a military Identification card when accepting an APO or FPO address.

- For a commercial entity the street address of the principal place of business, local office or other physical location. (According to CIP, a PO Box alone will not be acceptable.) If a business has multiple physical locations, the bank may obtain the physical address of each location or may accept the address of the company’s business office. Ask your BSA officer which your bank requires
Government-issued identification number

U.S. person
An acceptable identification number for U.S. persons may include a taxpayer identification number such as a Social Security number (SSN), or an Employer Identification number (EIN).

Non-U.S. person
For non-U.S. persons, the regulations recognize that while they may not be eligible to have a Social Security number (SSN), the bank may use other government-issued identification numbers. Each bank’s CIP may elect to accept all or only selected identification numbers for non-U.S. persons.

An acceptable identification number for non-U.S. persons includes the following items:

- A taxpayer identification number
- An Individual Taxpayer Identification number (ITIN)
- A passport number and country of issuance
- An alien identification card number
- A number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard

Date of birth
Banks should compare the date of birth on the driver’s license, passport, or alien identification card to the date of birth provided at account opening and compare the documented age to the physical appearance of the customer.

Note: If an individual or business attempts to open an account without the required information discussed above, the bank should not open the account or book the loan until the bank obtains that information.

Glossary terms

U.S. person
A United States citizen (including a naturalized citizen) or an entity created under the laws of a state or the United States such as a corporation, partnership, or trust.

Non-U.S. person
Anyone who does not meet the definition of a U.S. person.
CIP: Two-Step Process

Step two
Once the bank has gathered the identifying information, the bank must verify the customer’s identity. This is the second step in the process. It is important to understand that verification does not mean the bank must verify each and every piece of information. Instead, CIP allows the bank to establish procedures designed to let the bank form a reasonable belief that it knows the true identity of each customer.

Documentary and nondocumentary methods
Each bank has a choice of using what are known as documentary or nondocumentary methods to conduct its verification of the customer’s identity. Generally, each bank’s CIP will guide its employees regarding the methods that bank employees may use and under what circumstances employees may use different methods of verification. While the regulations have guidelines, each bank makes a decision about the types of documentation it will accept to verify a customer’s identity.

On most occasions involving an in-person account opening, the customer, especially individuals, must have a readily available and acceptable form of identification, such as a driver’s license, that makes verification easy. In account openings conducted online or over the telephone or where common forms of ID are not in the possession of the customer, verification may need to rely on nondocumentary methods consistent with your bank’s CIP policies and procedures.

» Click each tab to learn more about documentary and nondocumentary methods.
CIP: Two-Step Process

Documentary
If a bank uses documentary methods to verify a customer’s identity, the bank’s CIP will set the minimum acceptable documentation. The CIP rule gives the following examples of types of documents that have long been considered primary sources of identification:

- For an individual, the bank should obtain an unexpired, government-issued form of identification that provides evidence of the customer’s nationality or residence and that bears a photograph or similar safeguard; examples include a driver’s license or passport.
- For a person other than an individual (such as a corporation, partnership, or trust), the bank should obtain documents showing the legal existence of the entity, such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

> Roll over each source of documentary identification to see the procedures.

Photo ID
If the bank is using a photo ID to verify the customer’s information, what should bank employees look for?

- Does the person opening the account look like the person in the photo?
  If the person sitting at the CSR’s desk has grey hair and the picture shows someone with brown hair, it could just be an old picture, but if the license shows an 80-year-old man and the person 18 with acne, then that should alert the bank to a problem.
- Does the physical description match?
  If the person on the license is listed as being 6’2” tall with brown hair and blue eyes, and the person at the account opening desk is 5’3” tall, bald and brown eyes that should be a “red flag.”
- Does the address match? If not, why not?
  Has the person recently moved? Does the person have anything (utility bill, lease, credit card statement) matching the address the person is using to open the account?
- If the license or other photo ID contains a Social Security number, does it match the one provided by the customer?
Business documents
If the bank is using business documents to establish the identity of the business, be sure to take the following actions:

- Confirm that the EIN matches the one provided
- Confirm that the person is listed on the documents or on a letter from the Board of the corporation as the individual authorized to transact business on behalf of the entity
- Confirm that the entity is licensed or authorized to do business in the state
- Confirm that the business name on the document matches the name provided; a bank can verify this with the Better Business Bureau and/or the Secretary of State’s office in the state where the business is registered or is doing business
- Ask to see the document or letter granting tax exempt status such as a 501(c)(3) (or other tax exempt status) from the IRS, if the business is a charity

Click each tab to learn more about documentary and nondocumentary methods.

Sidebar

Minimum acceptable documentation

A bank’s CIP should be flexible enough to include methods of verification for people who are elderly or disabled and who do not or cannot have driver’s licenses. These methods can include state-issued ID card or other forms of valid ID. Bank employees should ask their supervisor if their bank makes any exceptions and what those exceptions are.
CIP: Two-Step Process

Documentary, continued

Prior to 2018, many states made it illegal for anyone to make copies of state-issued drivers’ licenses and identification cards. This made it very difficult for individuals to open accounts using online access. In 2018, Congress passed S2155: The Economic Growth, Regulatory Relief, and Consumer Protection Act.

» Roll over the image to learn more about S2155.

S2155: The Economic Growth, Regulatory Relief, and Consumer Protection Act

Section 213 of this law addresses online account opening and allows a customer to submit a copy of documentary identification. The purpose of this rule is to allow people living in states where copying state-issued IDs is illegal to open accounts online. That is where it begins and ends.

The rule allows the bank to retain a copy of the INFORMATION from the copy of the driver’s license or ID card, but banks may not retain a copy of the actual document. Language in the act indicates that banks are required to delete the copy or image of the customer’s personal identification after using it to for one of the following purposes:

1. Verifying the identity of the individual;
2. Verifying the authenticity of the driver’s license or personal ID; and
3. Complying with a legal requirement to record, retain or transmit the personal information in connection with opening an account or offering a financial product/service such as the BSA’s CIP requirements.

Unless federal BSA laws require the bank to keep a copy or image of a customer’s ID, the bank must permanently destroy this copy/image after using it for one of these three purposes.

The requirement to delete the photocopy of the ID applies only to online account opening. It does not apply to accounts or services requested in person at a branch. In addition, it applies only to deletion of the copy of the ID itself- not the information obtained from the ID. It also applies only in a BSA context and no other.
Current BSA laws do not require the retention of a copy/image of the ID. The BSA only requires banks to "record a description of any documents that were relied on, noting the type of document, any identification number contained in the document, the place of issuance and, if any, the date of issuance and expiration date" rather than the scanning or copying of a customer's ID. For those reasons, if the account, service or product requested online requires the customer's ID for verification purposes, the bank must permanently delete this record after using it for those purposes.

This law applies only to state-issued IDs and licenses. Federal law still prohibits requiring copies of federal government IDs or military IDs for ANY purpose.

» Click each tab to learn more about documentary and nondocumentary methods.
CIP: Two-Step Process

Nondocumentary
Banks are not required to use nondocumentary methods to verify a customer’s identity, but most banks do use a combination of both documentary and nondocumentary methods as ways to verify the information provided by the customer. However, a bank using nondocumentary methods must have procedures that set forth which methods the bank will use.

Verification
The bank’s identity verification procedures have been established to ensure the validity of a customer’s information provided on the deposit or lending application. Bank employees may use a combination of positive, negative, and logical verification methods.

» Roll over the image to see some of the nondocumentary verification methods banks and bank affiliates may use.

Nondocumentary verification methods
- A bank representative may mail “Welcome Letters” to all new deposit account customers each month. Any letter returned for an invalid address should be investigated
- An insurance representative will mail a life insurance quote to any individual requesting the quote
- Make a telephone call after the account relationship is opened or established
- Ask for paystubs to verify employment
- Obtain updated financial statements
- Compare the identifying information provided by the customer against fraud and bad check databases to determine whether any of the information is associated with known incidents of fraudulent behavior (negative verification)
- If mailings of coupon books, account statements, or tax escrow notices are returned to the bank for an insufficient or incorrect address, this should be researched and documented
- Compare the identifying information with information available from a trusted third party source, such as credit bureaus, security and demographic databases, and government databases (positive verification)
- Analyze whether there is logical consistency between the identifying information provided, such as the customer’s name, street address, ZIP code, telephone number, date of birth, and Social Security number (logical verification)
- Utilize government and/or Internet databases to verify business entity licensing and authorized signers
- Check bank references or ask to see bank statements from a prior bank

» Click each tab to learn more about documentary and nondocumentary methods.
Lack of verification

Each bank’s CIP must have procedures for circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. These procedures should describe the following requirements:

- Circumstances in which the bank should not open an account
- The terms under which a customer may use an account while the bank attempts to verify the customer’s identity
- When the bank should close an account, after attempts to verify a customer’s identity have failed
- When the bank should file a Suspicious Activity Report (SAR) in accordance with applicable law and regulation

When a business entity opens an account, the entity and not the individual signers is considered the “customer” for purposes of CIP. In some cases, however, just performing CIP on the business is not sufficient. This is true in the case of a high risk business such as a money services business or any business defined as inherently high risk by either the bank or the BSA.

In addition, a bank’s CIP must address situations where, based upon the bank’s risk assessment of a new account opened by a business, the bank will require information about individuals with authority or control over the account (signatories or authorized signers) in order to verify the customer’s identity. In other words, a CIP must address the situation when a non-individual opens an account, identity is suspicious, and the financial institution needs to look beyond the entity-owner to the individuals authorized to act on behalf of the entity. This extends to beneficial owners of legal entity customers as well.

CIP: Two-Step Process

Lack of verification

Each bank’s CIP must have procedures for circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. These procedures should describe the following requirements:

- Circumstances in which the bank should not open an account
- The terms under which a customer may use an account while the bank attempts to verify the customer’s identity
- When the bank should close an account, after attempts to verify a customer’s identity have failed
- When the bank should file a Suspicious Activity Report (SAR) in accordance with applicable law and regulation

When a business entity opens an account, the entity and not the individual signers is considered the “customer” for purposes of CIP. In some cases, however, just performing CIP on the business is not sufficient. This is true in the case of a high risk business such as a money services business or any business defined as inherently high risk by either the bank or the BSA.

In addition, a bank’s CIP must address situations where, based upon the bank’s risk assessment of a new account opened by a business, the bank will require information about individuals with authority or control over the account (signatories or authorized signers) in order to verify the customer’s identity. In other words, a CIP must address the situation when a non-individual opens an account, identity is suspicious, and the financial institution needs to look beyond the entity-owner to the individuals authorized to act on behalf of the entity. This extends to beneficial owners of legal entity customers as well.
CIP: Two-Step Process

Self Check Quiz
What are three acceptable identification numbers for a non-U.S. person?

» Select the correct answers and click Submit.

- A) A taxpayer identification number
- B) An Individual Taxpayer Identification number (ITIN)
- C) A passport number and country of issuance
- D) A library card

A, B, and C are correct.

D is incorrect because a library card is not generally considered to be an acceptable form of ID.
CIP: Two-Step Process

Self Check Quiz

Verification can be performed using which two methods?

» Select the correct answers and click Submit.

- A) As needed
- B) Documentary
- C) Nondocumentary
- D) Negative

B and C are correct.
A and D are incorrect because they are not methods of verification.

Page 15
CIP: Two-Step Process

Self Check Quiz

What are two acceptable documentary forms of identification?

» Select the correct answers and click Submit.

- A) Driver’s licenses
- B) Credit reports
- C) Passports
- D) Follow-up calls

A and C are correct.

B and D are incorrect because they are examples of nondocumentary verification methods.
Recordkeeping Requirements

Banks must implement reasonable procedures for maintaining records of the information used to verify a person’s name, address, and other identifying information are required under CIP.

When the bank relies on a document to verify identity, the bank employee must either maintain a copy of the document the bank relied on that clearly evidences the type of document and any identifying information it may contain OR record all identifying information about a customer including the following descriptions of any document:

- The type of document
- Any identification number contained in the document
- Place of issuance
- Dates of issuance and expiration

**Warning**: IMPORTANT: Many banks make a copy of the photo ID used as identification. While this may be useful at the teller line for identification purposes, the CIP has never required that photo IDs be copied or that a financial institution retain copies of the ID. The CIP does require banks to record the INFORMATION from any document relied upon when identifying the customer.

If the bank retains copies of identifying documents bearing photos such as a passport or a driver’s license, care should be taken to keep such information separate from loan files. Additionally, as noted earlier in this course, the federal government prohibits copying and retaining U.S. Government IDs such as military IDs, and some states have other restrictions on retaining copies of identifying documents for accounts opened in person. Ask your BSA officer about any state restrictions.
The bank must also record the methods and result of any additional measures undertaken to verify the identity of the customer. If the bank relies on documentation other than a government-issued identification to establish customer identity, the bank’s records must contain the following descriptions (or a copy) of any document upon which the bank or affiliate relied in order to verify the identity of the customer:

- The type of document, such as a phone bill, lease, partnership agreement
- Identification number (if applicable)
- Place of issuance, or entity issuing
- Dates of issuance and expiration (if applicable)

The bank must record the description of methods and results of any measures undertaken to verify the identity of the customer and the resolution of any discrepancy in the identifying information obtained.

The bank must retain records of name, address, date of birth (DOB), and EIN/TIN for five years after the date the account is closed. Records of documents used to verify identity, such as driver’s license or business records, must be retained for five years after the record is made.
Recordkeeping Requirements

**Question**
What two record retention options does the bank employee have when the bank relies on a document to verify identity?

**Answer**
Maintain a copy of the document the bank relied on that clearly evidences the type of document and any identifying information it may contain OR record all identifying information about a customer.
Reliance on Other Parties

Banks may rely on other financial institutions or third parties to provide information under CIP. There is a difference in the reliance provisions of the CIP between reliance on other financial institutions and reliance on third parties.

Other financial institutions
A bank or its affiliates may contract with other financial institutions to provide information under their CIP for any joint or shared customers. In these cases, the bank or its affiliates will engage in services, dealings, or other financial transactions only in the following situations:

- Such reliance is reasonable under the circumstances
- The other financial institution is subject to be examined under BSA
- The other financial institution is regulated by a Federal functional regulator
- The other financial institution enters into a contract certifying annually to the bank and its affiliates that it will perform the specified requirements of the CIP program (or their own procedures but only in cases where their procedures are more stringent)
Use of third parties
Under the CIP rules, a bank is allowed to use a third party such as an agent or service provider to perform services on its behalf. Therefore, a bank is permitted to arrange for a third party, such as a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer. 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. The bank is ultimately responsible for that third party’s compliance with the requirements of the bank’s CIP.

As a result, banks should establish adequate controls and review procedures for such relationships. This requirement is different from the reliance provision of the rule that permits the relied-upon party to take responsibility.

Reliance on Other Parties
Use of third parties
Under the CIP rules, a bank is allowed to use a third party such as an agent or service provider to perform services on its behalf. Therefore, a bank is permitted to arrange for a third party, such as a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer. 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. The bank is ultimately responsible for that third party’s compliance with the requirements of the bank’s CIP.

As a result, banks should establish adequate controls and review procedures for such relationships. This requirement is different from the reliance provision of the rule that permits the relied-upon party to take responsibility.
Reliance on Other Parties

Question
If the bank is extending credit to the borrower using a car dealer or mortgage broker as its agent, who is responsible for performing the bank’s CIP?

Answer
If 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.
Self Check Quiz

CIP applies to the identification of customers and is the first step in conducting customer due diligence. What are two tasks included in establishing customer identity?

» Select the correct answers and click Submit.

- A) Send all customer information to law enforcement
- B) Collect a business or personal address for the customer
- C) Require the customer to be a U.S. citizen
- D) Use government-issued documents or other reliable means to verify the customer’s identity

B and D are correct.

A is incorrect because sending all customer information to law enforcement is not part of a bank’s identification or due diligence process. C is incorrect because a customer does not have to be a U.S. citizen.

B and D are correct.
Customer Identification and Account Opening

CIP notice
According to the USA PATRIOT Act, the law that mandates the CIP, banks must inform customers that specific information is required when opening a new account. The final rules for CIP provide banks with model disclosure language. This disclosure may be located on advertising materials, on counters or desks where there is customer contact, and every place in a bank where employees open new accounts, including lending, trusts, or investments. It may also be posted on each bank’s application forms, on a bank’s Internet site, and even on doors leading into a branch location. Often bank employees who open accounts on the phone are instructed to give the notice verbally.

Review the wording in this sample USA PATRIOT Act notice.

Important Information You Need to Know About 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 individual or business that 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 allows us to identify you. We may also ask to see your driver’s license or other identifying documents.
Customer Identification and Account Opening

The notice may be handled in the following ways:

- **Branches**—Notice signage placed in each branch. The notice may also be available as part of the Deposit Account Agreement, and should be given in paper form to anyone taking information outside the branch for another signor (i.e., joint signers where all are not present at the account opening).
- **Telephone**—Clients who open accounts over the telephone may receive the notice verbally.
- **Personal loans**—The notice may be provided using a paper form, may be placed on the loan officer’s desk, or may be added to any loan applications used by the bank.
- **Online deposit and loan applications**—The bank should provide the notice on its website and/or included with any disclosures mailed to an applicant.
- **Mortgage**—The notice can be mailed to the customer as part of the initial loan disclosures (Loan Estimate) or the bank can provide it at closing when the bank obtains verifying documentation.
- **Federal student loans**—Sallie Mae provides a notice in accordance with CIP guidelines.
- **Commercial loans**—The bank should provide this notice as part of the proposal and/or the commitment letters.
Customer Identification and Account Opening

Responding to customer questions and concerns

When a customer establishes a relationship with a bank—or whenever a customer opens a new account—the bank is required to obtain specific identifying information from the customer.

Even though the PATRIOT Act notice discussed previously may be prominently displayed on a banker’s desk, customers may have questions and concerns.

Note that these types of concerns are likely to arise any time you are requesting confidential personal information from a customer, such as for wire transfers, sales of negotiable instruments or even the completion of a CTR. The important thing to remember is that this information is required by federal law, and although the customer has the right not to provide it, the bank, faced with such a refusal, must decline to conduct the transaction or open the account.

Remember, too, that not all requirements grow out of the law; some are bank policy. For example, the CIP does not require that banks obtain personal information (date of birth, SSN, and address) on signers on a commercial account unless that account is high risk, such as a money services business account. (Or unless the signer is a beneficial owner or control person on a commercial account.) However, some banks do require this information on all signers on business accounts as a matter of bank policy. The CIP is risk-based, so the decision to obtain more information than is required by law is one that a bank’s BSA officer in conjunction with the bank’s board of directors has determined best meets the bank’s requirements. Therefore, bank employees must adhere to those rules, as each bank must abide by its own policy.
Customer Identification and Account Opening

Exercise

Instructions
Read the customer scenario and script. Type what you would say to respond to this customer's questions and concerns.

Scenario 1
Earl has approached your bank and asked to open a checking, money market, CD, and an overdraft line of credit. You welcome him to the bank, but as you begin the account opening process, Earl balks at providing his Social Security number. Earl is a bit of a conspiracy theorist and really does not see why he needs to provide this information just to have a bank account. Other than the fact that you need Earl's Social Security number to pull a credit report in order to honor his request for credit, how would you respond to Earl?

» Type your answer in the field. When finished, click the Suggested Results button to view a possible response.

Suggested Results
To prevent financing of terrorist operations and money laundering, federal law requires each bank to implement Customer identification programs (CIPs). The requirements go beyond just verifying your identity. Banks must now keep records of identifying information and check customer names against terrorist lists. This applies to anyone who opens a new account. So, if you open a personal account, then your SSN is required. If you open a business account, then the businesses’ EIN is required. Be assured that our bank protects your Social Security number and any other personal information you provide to us. We operate under a rigorous, board approved information security program that is subject to examination and oversight, and only those who need to know a customer's financial information—because they provide the accounts and services the customer might need—are authorized to have access to it.

Page 27
Customer Identification and Account Opening

Question
How is the USA PATRIOT Act notice handled when clients open an account at a branch?

Answer
Notice signage is placed in each branch. The notice may also be available as part of the Deposit Account Agreement and should be given in paper form to anyone taking information outside the branch for another signer (i.e., joint signers where all are not present at the account opening).

Page 28
Wrap Up

By completing BSA/AML: CIP Basics, you learned what constitutes an account and a customer under the CIP rule. You also learned what actions to take in the two-step process of obtaining identifying information and verifying the identity of the customer. You can now identify the procedures for maintaining records of the information used to verify a person's name. You also know the established controls and review procedures for reliance on other parties. In addition, you can now identify methods for handling the CIP notice at account opening.

» Click Exit to close this course.

Page 29