Compliance for Deposit Operations

Customer Due Diligence

Pennsylvania Association of Community Bankers

November 2020

Consultants to the Financial Industry
Young & Associates, Inc.
121 E. Main Street
P.O. Box 711
Kent, OH 44240

Phone: 330.678.0524
Fax: 330.678.6219
www.younginc.com

Table of Contents

Section 1: Introduction

Introduction

In recent years, the banking regulators have required banks to perform some level of Customer Due Diligence (CDD). They have now made CDD the fifth pillar of BSA. The expectations concerning CDD were specified in the *Exam Manual*. The opening paragraphs of this section of the *Exam Manual* states:

> "The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of comprehensive CDD policies, procedures, and processes for all customers, particularly those that present a high risk for money laundering and terrorist financing. The objective of CDD procedures should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage. These procedures assist the bank in determining when transactions are potentially suspicious. The concept of CDD begins with verifying the customer's identity and assessing the risks associated with that customer. Procedures should also include enhanced CDD for high-risk customers and ongoing due diligence of the customer base.
>
> Effective CDD policies, procedures, and processes provide the critical framework that enables the bank to comply with regulatory requirements and to report suspicious activity. An illustration of this concept is provided in Appendix K ("Customer Risk Versus Due Diligence and Suspicious Activity Monitoring").
>
> CDD policies, procedures, and processes are critical to the bank because they can aid in:
>
> - Detecting and reporting unusual or suspicious transactions that potentially expose the bank to financial loss, increased expenses, or reputation risk.
> - Avoiding criminal exposure from persons who use or attempt to use the bank's products and services for illicit purposes.
> - Adhering to safe and sound banking practices."

Developing a CDD program should not be a "one size fits all" approach. Although many banks have similarities, all banks vary in the level of inherent risk, based on customer base, products, services, and geographies. Therefore, CDD programs will vary from bank to bank.

Customer Due Diligence (CDD) Rule

There are four core elements of CDD as follows:

1. customer identification and verification,
2. beneficial ownership identification and verification,

3. understanding the nature and purpose of customer relationships to develop a customer risk profile, and
4. ongoing monitoring for reporting suspicious transactions and, on a risk-basis, maintaining and updating customer information.

The first element is implemented through a bank's Customer Identification Program (CIP). The second element is the most recent, and is required by the final FinCEN rule. The third and fourth elements are required for covered financial institutions to comply with their suspicious activity reporting requirements. The AML program rules for all covered financial institutions are being amended by the final rule in order to include the third and fourth elements as explicit requirements.

The biggest change that occurred in 2018 is the requirement to ***identify*** and ***verify*** the individuals who own or control the bank's legal entity customers (also known as beneficial owners) when opening new accounts (both deposits and loans). Existing customers will be impacted only when they open a new account.

These rules only apply to legal entity customers, which means that it will not affect individual accounts and other exceptions and exclusions (such as sole proprietors, publically traded companies, government agencies, most trusts, and other similar entities).

Beneficial Owner Definition

A "beneficial owner" is defined as having two prongs: 1) the ownership prong; and 2) the control prong. The ownership prong includes each individual, if any, who directly or indirectly owns 25 percent of the equity interests of a legal entity customer while the control prong includes a single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager or any other individual who regularly performs similar functions.

Identification

To ***identify*** ultimate beneficial owners, our bank will provide a Certification Form to each individual opening a new account on behalf of a legal entity (business). This Certification Form will be collected in a manner substantially similar to what we currently do in requiring a Corporate Resolution from each business. In completing the Certification Form, the individual representing the business will provide us with the names of the ultimate beneficial owners of the business. We are not required to verify that the provided information is correct as we can rely on the information provided to us.

Verification

Once an ultimate beneficial owner is identified, we must then ***verify*** their identity by requiring the same elements from them that we require from an individual opening a new account. This includes core CIP information (Name, date of birth, address, and SSN), documentary identification (driver's license) and nondocumentary identification (like ChexSystems). We do not have to get this information directly from the beneficial owner, but are permitted to get it directly from the individual opening the new account on behalf of the business.

Customer Due Diligence (CDD) Overview (Excluding Beneficial Ownership)

The foundation of strong BSA/AML programs is the implementation of complete CDD policies, procedures, and controls for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The concept of CDD builds upon the CIP regulatory requirements for identifying and verifying a customer's identity.

The goal of a CDD program is to develop an awareness of the unique financial details of the institution's customers and the ability to predict the type and frequency of transactions in which its customers are likely to engage. In this way, institutions can better identify, research, and report suspicious activity as required under BSA. Although customer due diligence is not required by statute or regulation, an effective CDD program is the framework that allows the institution to comply with regulatory requirements.

Benefits of an Effective CDD Program

An effective CDD program protects the reputation of the institution by:

- Preventing unusual or suspicious transactions that would expose the bank to loss or expense
- Helps the bank avoid criminal exposure by those who would use the bank for illegal activity
- Ensuring compliance with BSA regulations and holding to sound banking practices.

Another way to realize the benefits of an effective CDD program is through the following:

- Using a customer risk rating system to allocate bank resources for monitoring purposes
- Focusing the majority of the bank's monitoring efforts on those customers that present the greatest risk
- Compliance with the BSA through a risk-based approach.

CDD Program Guidance

CDD programs should be tailored to each institution's BSA/AML risk profile; consequently, the scope of any CDD program will vary. Even though a small bank may have more frequent direct contact with customers than those at larger banks, all financial institutions should adopt a CDD program.

An effective CDD program should:

- Be in proportion to a banks BSA/AML risk profile,
- Be clear in management's expectations and staff responsibility, and
- Establish monitoring systems and procedures to identify activity that is inconsistent for a customer's normal banking activity.

Elements of a CDD Program

While there is a great deal of flexibility allotted to banks in devising an appropriate CDD program, all Know Your Customer programs should contain certain critical features, which are discussed below. Each program should also delineate acceptable documentation requirements and the due diligence procedures the bank will follow. The delineation of this information in the CDD program will ensure that the same standards are applied throughout the bank and will inform auditors and examiners of the bank's established standards for review of customer information.

Minimum Steps for Compliance

The following are the minimum steps the banks should take in order to comply with the CDD expectations.

Identify the Customer

The USA PATRIOT Act, Section 326 made a provision part of the law to identify the "true" identity of a customer. The rule for customer identification was discussed earlier in this manual.

Determine the Source of Funds

The CDD program should provide a system for determining the source of a customer's funds. The amount of information needed to do this can depend on the type of customer in question. As an example, if a retail banking customer maintains demand deposit accounts funded primarily from payroll deposits, it should be a relatively simple task to identify and document the source of funds as payroll deposits. On the other hand, a more detailed analysis, with a more extensive documentation process, would be required for high net worth customers with multiple deposits from a variety of sources.

For these reasons, among others, it may be beneficial for banks to classify customers into varying categories, based on factors such as the types of accounts maintained, the types of transactions conducted, and the potential risk of illicit activities associated with such accounts and transactions. Banks could then develop procedures to obtain necessary information and documentation based on the risk assessment for the various categories or classes established by a bank.

Determine Normal and Expected Transactions

The CDD program should provide a system for determining a customer's normal and expected transactions involving the bank. Without this information, a bank is unable to identify suspicious transactions. A bank's understanding of a customer's normal and expected transactions should be based on information obtained both when an account is opened and during a reasonable period of time afterward. It also should be based on normal transactions for similarly situated customers.

Monitor the Account Transactions

The CDD program should provide a system for monitoring, on an ongoing basis, the transactions conducted by customers and identifying transactions that are inconsistent with the normal and expected transactions for particular customers or for customers in the same or similar categories or classes. The examiners do not require that every transaction of every customer be reviewed. Rather, they do expect a bank to develop a monitoring system that is appropriate for the risks presented by the accounts maintained at that bank.

In designing a monitoring system, a bank may choose to classify accounts into various categories based on factors such as the type and size of account; the types, number, and size of transactions conducted in the account; and the risk of illicit activity associated with the account. For certain classes or categories of accounts, it would be sufficient for an effective monitoring system to establish parameters for which the transactions within these accounts will normally occur. Rather than monitoring each transaction, an effective monitoring system could entail monitoring only for those transactions that exceed the established parameters for that particular class or category of accounts. For other categories or classes of accounts, such as private banking accounts, it may be necessary to monitor each significant transaction.

Determine If the Transaction Should Be Reported

Once a transaction is identified as inconsistent with normal and expected transactions, the bank must determine if the transaction warrants the filing of a Suspicious Activity Report. In identifying reportable transactions, a bank should not conclude that every transaction that falls outside what is expected for a given customer should be reported. Rather, a bank should focus on patterns of inconsistent transactions and isolated transactions that present risk factors that warrant further review.

Customer Risk

A bank is expected to identify and understand its money laundering and terrorist financing risks of the bank's customer base. The most efficient method to understand the ongoing risks is to obtain appropriate and relevant information at account opening. Such information should be sufficient enough to allow the bank to develop an understanding of normal and expected activity for the customer's occupation or business operations.

As part of an institution's BSA/AML risk assessment, many institutions apply a BSA/AML risk rating to its customers. Using this approach, the institution will gather enough information at account opening to develop a customer transaction profile to understand what will be expected activity for that customer's occupation or business. The following from the *Exam Manual* addresses the risk-based approach a bank should follow when risk rating and monitoring customer activity:

> "This information should allow the bank to differentiate between lower-risk customers and higher-risk customers at account opening. Banks should monitor their lower-risk customers through regular suspicious activity monitoring and customer due diligence processes. If there is indication of a potential change in the customer's risk profile (e.g., expected account activity, change in employment or business operations), management should reassess the customer risk

rating and follow established bank policies and procedures for maintaining or changing customer risk ratings.

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

CDD processes should include periodic risk-based monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g., change in employment or business operations)."

Assigning a risk rating to customers may not be appropriate for all banks, but bank management should have a detailed understanding of money laundering and terrorist finance as well as knowing their customer base to limit risk.

Assessing Risk

In general, customers may pose low-risk or high-risk or some combination in between.

Examples of low risk (routine or usual accounts) include:

- Low aggregate balances
- Low volume of activity
- Household accounts
- Most retail passbook savings/checking accounts
- Accounts for minors

Examples of higher-risk accounts or activities includes:

- Large balances
- High volume of activity
- Frequent or excessive funds transfers
- Frequent or excessive large cash transactions

Personal Accounts. When opening personal accounts, banks may want to consider the following:

- Location of residence
- Follow-up calls
- Source of funds (especially large sums of cash)
- For larger accounts, prior bank references are recommended
- Checking with service bureaus (i.e., ChexSystems)

Business Accounts: In addition, consider the following when opening business accounts, as applicable:

- Evidence of customer's legal status
- Article of incorporation, partnership agreement, etc.
- Certificate of Good Standing with state
- Business license
- Check with reporting agency (i.e., Dunn & Bradstreet, etc.)
- Prior bank references
- Follow-up calls and on-site visits
- Source of funds
- Description of line of business
- For larger accounts:
- Financial statements
- Listing of major suppliers, customers, and geographic locations
- Description of business's primary trade area
- Whether international transactions are expected
- Description of business operations (i.e., retail vs. wholesale)
- Anticipated volume of cash activity

High-Risk Products and Services

While a bank may have additional high risk products and services, three forms of possible high-risk products or services are presented here:

- Wire transfer/International Correspondent Bank Accounts
- Private Banking Relationships, and
- Electronic Banking

Wire Transfer/International Correspondent Bank Accounts. When dealing with wire transfers or international accounts, banks should consider the following factors:

- Account purpose
- Location of foreign bank, if applicable
- Nature of banking license of correspondent bank
- Correspondent's AML program
- Prevention controls

- Extent of banking regulation enforced in the foreign country

For our typical domestic based customers, wire transfer activity can pose an issue if the purpose or frequency of the funds transfer activity is not reasonable for the type of customer or the customer's business. Therefore, it is important to determine the level of any funds transfer activity of a prospective customer at the time of account opening and continually monitor such activity to ensure that it falls in line with the original expectations. One simple method to accomplish this objective is to inquire at account opening the following:

- Does the customer perform funds transfers?
- What will be the expected frequency and amounts of such transfers?
- Does the customer deal with international suppliers or customers?
- Obtain a list of such suppliers and customers
- Ensure that none appear on any sanctioned lists (i.e., OFAC)
- Does the customer deposit currency and then subsequently wire funds out of the bank on a regular basis?

Depending on the answers to the above, there may be some initial high-risk concerns by the bank if the customer is dealing in a high level of funds transfer activity, especially on an international basis.

Private Banking Relationships. Private banking is generally considered the personal or discreet offering of a wide variety of financial services and products to the affluent market. It can involve customers as individuals, commercial businesses, law firms, investment advisors, trusts, etc. Proper due diligence when opening private banking accounts goes beyond the normal procedures or controls employed with a bank's typical retail customer base. Items to consider when opening private banking accounts includes:

- Confirming references
- Background checks
- Determining the source of the client's wealth, needs and expected transactions

Electronic Banking. Electronic banking is a broad term that encompasses a variety of delivery channels: telephone banking, Internet banking, PC-base banking, ATMs and ACHs. In today's environment, electronic banking is becoming more and more popular given our hectic lifestyles. While most customers that utilize electronic banking channels to conduct transactions do so in a legitimate manner, the mere existence of such channels has raised concerns by the regulators. In general, electronic banking is vulnerable to money laundering and terrorist financing due to user anonymity, rapid transaction speed and its wide geographic availability. When offering electronic banking channels, banks should consider the following:

- Customer's proximity to the bank's branches
- Requirement for the customer to initiate electronic banking services on-site at the bank
- Review of customer's transactions and expected transactions

High-Risk Customers

Financial institutions are expected to develop a high-risk customer list from their customer base. While included in Section 2 of this manual, the following is reproduced as a reminder of those types of entities that are considered as possessing a higher degree of risk:

- Cash intensive businesses such as convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators and parking garages
- Pawn brokers
- Purchasers or sellers of any type of motor vehicle, vessel, aircraft, farm equipment or mobile home
- Auctioneering
- Chartering or operation of ships, buses or aircraft
- Gaming of any kind
- Trade unions
- Title insurance operations and real estate closing
- Professional service providers such as doctors, attorneys, accounts and real estate brokers
- Non-governmental organizations and charities
- Non-bank financial institutions, which would include money service businesses (MSB), casino and card clubs, brokers/dealers in securities, and dealers in precious metals, stones and jewels
- Senior political figures, their immediate families and close associates (PEPs)
- Non-resident aliens and accounts of foreign individuals
- Foreign corporations maintaining transactions accounts, offshore corporations, and international business corporations located in high-risk geographic areas
- Deposit brokers (including foreign brokers)
- Foreign financial institutions, including banks and foreign money service providers

Once identified, the bank can determine which customers are conducting transactions and/or using services of the bank that would warrant remaining on a high-risk list and necessitate further monitoring.

High-Risk Geographic Locations

Identifying high-risk geographic locations is essential to a bank's anti-money laundering program. A condensed reminder of those available resources of high-risk geographic locations is as follows:

- Jurisdiction identified by intergovernmental organizations (e.g., FATF)

- Countries/jurisdictions identified by the US Department of State's International Narcotics Control Strategy Report (INCSR)
- Geographies identified by OFAC
- Jurisdictions designated by the Secretary of the Treasury as being primary money concern as authorized by the USA Patriot Act
- Jurisdictions identified by bank management

Risk Codes

A customer risk rating system should be developed before a bank may begin assigning risk ratings to its customers. Risk rating systems can range from the most simplistic to highly sophisticated. Given the wide variety of bank sizes, types, customer bases and locations, there is no one perfect method for every bank. Below are two different approaches.

The following is a modification to various risk rating systems that have been utilized by banks and regulators alike. On the surface, this rating system is rather simplistic and attempts to limit the number of risk levels. The levels of customer risk range from highest (1) to lowest (4).

1. High
   a. Customers where an SAR has been considered in the past
   b. Customers that fall into the high-risk categories for all three risk factors (i.e., customer type, products/services used, and location of customer)
2. Moderate High
   a. Customers that may not be exempted from CTR filings
   b. Customers that fall into the regulator identified high-risk customer and geographic category
   c. Non-U.S. citizens
   d. Customers that reside outside of a pre-defined radius of the bank's locations (i.e., 50 mile radius, outside of the county in which the bank operates, etc.)
   e. Customers where an SAR was considered or filed in the past and no subsequent suspicious activity has occurred in a pre-defined period of time (i.e., within 6 months following the initial suspicious activity)
3. Moderate
   a. Customers that did not provide sufficient information to verify identity at account opening
   b. Customers that fall into any one of the three regulator identified high-risk categories
4. Low
   a. Any customer that is not rated 1 through 3
   b. Risk Rating Existing Customer Base

Agreeing on a risk rating system or model might be considered simple when compared to the daunting task of assigning a rating to all existing customers. The following will discuss a logical approach to initiate the process and establish benchmarks that can be used for existing and new customers.

It is important to note that, when assigning risk ratings to specific customers, the bank must be cognizant that the various risk factors can interrelate. For example, a customer that might utilize a higher risk service may not result in a high-risk rating for that particular customer. The customer's profile should be considered in such situations. When assessing the existing customer base, the above risk rating code sample (or similar) should be referenced as ratings are assigned.

The assignment of responsibility to assign risk ratings is integral in a bank's overall CDD process. An effective risk rating process will have checks and balances, and allow for modification over time. Each institution will need to find a process that works best; however, the following are offered as suggestions in its development:

- *Initial risk rating options* –
  - Developing a comprehensive, user-friendly account opening form used by line staff, which guides staff on assigning initial ratings
  - Deferring the risk rating process to select individuals within the institution
- *Risk rating adjustments* – allowing for a post-review of risk ratings to assure that the rating system is properly employed
- *Account closure* – allowing for authority to close an account relationship should the risk rating prompt such action
- *Modifications to system* – allowing for adjustments to the risk rating system, as necessary

Step One: High-Risk Types. Begin the process by identifying those existing customers that fall into any of the customer type categories identified by regulators as high-risk. While this process can take time when reviewing a bank's existing customer database, it can be broken down into manageable pieces to expedite the process. For example, customers can be grouped into account types and assigned to designated staff to complete the assessment. The analysis of customers' geographic locations may present a problem since it is impractical to assess each and every customer's address, as compared to the listing of regulator-defined high-risk areas. A more practical approach is to first determine if any of the customer base resides, overlaps, or is adjacent to such areas. If the bank is located nowhere near such areas, then this part of the assessment should be minimal.

As part of the high-risk type analysis, the reviewer should identify any customers that engage in a business that is not eligible for a Phase II exemption.

Step Two: Suspicious Activity. Next, banks should identify any customers where suspicious activity reports (SARs) have been considered or filed in the past. Care should be taken on the final risk rating category assigned for these customers so that the risk rating does not readily highlight the fact that an SAR has been filed, since this information is to remain confidential. When bringing an assessment up-to-date, the reviewer might consider reviewing those instances where an SAR was filed or considered within a predefined time frame, such as during the most recent 12 months. Banks with effective suspicious activity monitoring programs should be able to rely on these procedures to readily identify those individuals of particular concern.

Step Three: High-Risk Products/Services. As a result of the bank products or services that have been identified as possessing a higher risk (which will be discussed in the next section,)

banks should next create a listing of the customers that utilize such products or services. This list of customers should then be cross-referenced with the other high-risk areas (i.e., customer type and geographic location).

Step Four: Customer Activity. Banks are afforded with a wealth of customer activity records. These records, including cash activity, can provide a significant amount of information about a customer's profile. Subject to system limitations, banks should utilize their databases to identify the following:

- **Cash Activity.** Customers that routinely engage in large currency transactions. The minimum thresholds for cash activity should be below the regulatory reporting amount of $10,000. In today's banking environment, many banks already track cash activity that is above $3,000 (or similar) to assist in their CTR reporting process and suspicious activity monitoring programs. As part of this process, banks need to become familiar with a customer's usual activity. If a wage earner customer (i.e., someone whose income is reported on a W-2) has frequent cash activity, then the bank needs to determine the source of the funds. While many bankers may be uncomfortable asking for customer explanations, the bank must, by whatever method, determine if the cash activity is normal or unusual.
- **Monetary Instrument Purchases.** The regulations require banks to record any sales of monetary instruments involving currency of $3,000 to $10,000, inclusive. These records, when reviewed periodically, can provide the bank with insight concerning any suspicious activity. Such records should be reviewed during the risk rating process to determine if any customers are frequently purchasing such instruments without any reasonable or legitimate purpose. A subset of this review might include reviewing where the instruments are cashed (i.e., in a foreign country) to determine if the risks need to be elevated.
- **Funds Transfers.** Since banks are required to record certain information about persons that originate or receive funds through the wire system involving amounts of $3,000 or more, these records can be used to identify customers or persons that conduct frequent transactions without any reasonable or legitimate purpose. These records should already be incorporated into an ongoing review by a bank's BSA officer or designee, which serves to determine whether frequent funds transfers by a particular customer meet his/her risk profile.

Step Five: Customer Location. A review should be performed to identify any customers that reside outside of the bank's predefined market area. It should be noted that some of these customers may not pose higher risks, but rather have relocated or have family connections to the market area. Customers that do fall into this category with no ascertainable reason to maintain an account at the bank require further evaluation. In addition, customers that are classified as non-U.S. persons will need to be identified.

Step Six: CIP Concerns. Finally, the reviewer shall identify those customers that have recently opened a customer relationship but have not fulfilled the bank's CIP requirements. Ideally, a designated person or department within the bank should be tracking such customers on an ongoing basis. Any customers that have failed to provide either identity or verification information should be flagged to allow the institution to track the fulfillment of CIP requirements. Depending on the bank's written CIP, eventually the bank should take appropriate action when CIP requirements are not met.

Monitoring

Once the customer base has been risk rated, the process of ongoing monitoring begins. Depending on each bank's resources, the level of available reports and/or tools will vary. However, even the smallest of institutions shall have methods employed to assess customer risks on an ongoing basis. In the simplest of examples, higher risk rated customers should be monitored more frequently than the low-risk customers. In addition, the types of monitoring reports for high-risk customers will likely contain transaction or customer profile specific parameters. For example, cash activity for "one" risk rated customers might be monitored for any cash activity of $3,000 and greater each business day. In addition, these same customers might be monitored for cash activity exceeding specific amounts over a designated time period (i.e., cash activity of $15,000 or more in a seven-day period).

When developing such monitoring methods, banks must first be cognizant of its higher risk customers and the tools available to effectively monitor the accounts. Not every bank will be expected to spend large sums of money or resources to implement such methods, but the methods should be commensurate with its overall risks.

Other High-Risk Resources

While examiners are frequently targeting a bank's policy and procedures addressing high-risk customers, activities and services during a BSA examination, there has not been an abundance of information to help guide banks on exactly how to deal with this area. There are a variety of resources available to assist us with high-risk activities.

One such valuable resource can be found in the OCC's publication Money Laundering: A Banker's Guide to Avoiding Problems (December 2002). It may be found on the agency's Web site at www.occ.treas.gov. Additional assistance can be found in the *Exam Manual*.

Section 11: Beneficial Ownership

Summary

FinCEN issued final rules under the Bank Secrecy Act to clarify and strengthen customer due diligence requirements for banks. The rules contain explicit customer due diligence requirements and include a requirement to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.

Effective Dates

The final rules were effective July 11, 2016. Banks were required to comply with these rules by May 11, 2018 (Applicability Date).

Executive Summary

Banks are not presently required to know the identity of the individuals who own or control their legal entity customers (also known as beneficial owners). This is viewed as a weakness of the system that they are trying to correct.

FinCEN believes that there are four core elements of CDD)

- customer identification and verification,
- beneficial ownership identification and verification,
- understanding the nature and purpose of customer relationships to develop a customer risk profile, and
- ongoing monitoring for reporting suspicious transactions and, on a risk-basis, maintaining and updating customer information.

Beneficial Ownership

Banks must identify and verify the identity of the beneficial owners of all legal entity customers (other than those that are excluded) at the time a new account is opened (other than accounts that are exempted). They may comply either by obtaining the required information on a standard certification form or by any other means that comply with the regulation.

Banks may rely on the beneficial ownership information supplied by the customer, provided that it has no knowledge of facts that would call into question the reliability of the information. The identification and verification procedures for beneficial owners are very similar to those for individual customers under a bank's customer identification program (CIP), except that for beneficial owners, the institution may rely on copies of identity documents. Banks are required to maintain records of the beneficial ownership information they obtain, and may rely on another

bank for the performance of these requirements, in each case to the same extent as under their CIP rule.

Anti-Money Laundering Program Rule Amendments

The AML program requirement for banks now explicitly includes 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.

A customer risk profile refers to the information gathered about a customer at account opening used to develop a baseline against which customer activity is assessed for suspicious activity reporting. This may include self-evident information such as the type of customer or type of account, service, or product. The profile may, but need not, include a system of risk ratings or categories of customers.

CDD also includes conducting ongoing monitoring to identify and report suspicious transactions and, to maintain and update customer information. For these purposes, customer information includes information regarding the beneficial owners of legal entity customers. The regulation requires that banks conduct monitoring to identify and report suspicious transactions. Because this includes transactions that are not of the sort the customer would be normally expected to engage, the customer risk profile information is used (among other sources) to identify such transactions. This information may be integrated into the bank's automated monitoring system, and may be used after a potentially suspicious transaction has been identified, as one means of determining whether or not the identified activity is suspicious.

When a bank 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. This applies to all legal entity customers, including those existing on the Applicability Date.

This provision does not impose a categorical requirement that banks 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.

Section-by-Section Analysis (Abridged)

Section 1010.230 Beneficial Ownership Requirements for Legal Entity Customers

Covered banks are required to establish and maintain written procedures reasonably designed to identify and verify the identities of beneficial owners of legal entity customers.

This requirement is separate from a policy objective of requiring States to obtain beneficial ownership information from the legal entities they create at the time of formation and upon specified circumstances thereafter. Presently, corporate laws and regulations differ from State to State, but generally do not require information regarding beneficial ownership. The information

provided significantly augment information presently available to law enforcement from State authorities, thereby improving the overall investigative, regulatory, and prosecutorial processes.

There is no categorical, retroactive requirement. However, the absence of a categorical mandate to apply the requirement retroactively would not preclude banks from deciding that collecting beneficial ownership information on some customers on a risk basis during the course of monitoring may be appropriate for their institution.

Section 1010.230(b) Identification and Verification

Section 1010.230(b)(1)

To facilitate banks' abilities to rely upon the Certification Form, the Certification Form includes a section that requires the individual opening the account on behalf of a legal entity customer to certify that the information provided on the form is true and accurate to the best of his or her knowledge.

The rule permits banks to use the Certification Form to collect beneficial ownership information. Banks must identify the beneficial owner(s) of each legal entity customer at the time a new account is opened, unless the customer is otherwise excluded or the account is exempted. Banks may accomplish this either by obtaining certification in the form from the individual opening the account on behalf of the legal entity customer, or by obtaining from the individual the information required by the form by another means, provided the individual certifies, to the best of the individual's knowledge, the accuracy of the information.

These records may be retained electronically and incorporated into existing databases as a part of overall management of customer files, and you will have flexibility in integrating the beneficial ownership information requirement into existing systems and processes. The certification of accuracy by the individual submitting the information may be obtained without use of the Certification Form in the same way the bank obtains other information in connection with its account opening procedures.

Banks generally have long-standing policies and procedures, based on sound business practices and prudential considerations, governing the documentation required to open an account for a legal entity; these typically include resolutions authorizing the entity to open an account at the institution and identifying the authorized signatories. Such resolutions are typically certified by an appropriate individual. It would be appropriate for the same individual to certify the identity of the beneficial owners.

While not requiring periodic updating of the beneficial ownership information of all legal entity customers at specified intervals, the opening of a new account is a relatively convenient and otherwise appropriate occasion to obtain current information regarding a customer's beneficial owners.

Section 1010.230(b)(2)

A covered bank 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 regulation requires that at a minimum, these procedures must contain the elements required for verifying the identity of customers that are individuals, but are not required to be identical. The rule clarifies that in the case of documentary verification, the bank may use photocopies or other reproductions of the documents listed in the CIP rule.

Because the risk-based verification procedures must contain the same elements as required by the applicable CIP rule to verify the identity of individual customers, verification must be completed within a reasonable time after the account is opened. The beneficial ownership identification procedures must address situations in which the bank cannot form a reasonable belief that it knows the true identity of the beneficial owner of a legal entity customer after following the required procedures.

Banks should conduct their own risk-based analyses of the types of photocopies or reproductions that they will accept in accordance with this section, so that such reliance is reasonable. As with CIP, banks are not required to maintain these copies or reproductions, but only a description of any document upon which the bank relied to verify the identity of the beneficial owner. Banks are not prohibited from keeping them in a manner consistent with all other applicable laws or regulations.

FinCEN generally expects beneficial ownership information to be treated like CIP and related information, and to be used to ensure that banks comply with other requirements. For example, the Office of Foreign Assets Control (OFAC) requires covered banks to block accounts (or other property and interests in property) of, among others, persons appearing on the Specially Designated Nationals and Blocked Persons List (SDN List), which includes any entity that is 50 percent or more owned, in the aggregate, by one or more blocked persons, regardless of whether the entity is formally listed on the SDN List.

Therefore, banks 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. Covered banks should also develop risk-based procedures to determine whether and/or when additional screening of these names through, for example, negative media search programs, would be appropriate.

FinCEN expects banks to apply existing procedures consistent with CTR regulations and applicable FinCEN guidance. While banks should generally recognize the distinctness of the corporate form and not categorically impute the activities or transactions of a legal entity customer to a beneficial owner, they must aggregate multiple currency transactions if the bank has knowledge that these 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. While the requirement to identify the beneficial owners of legal entity customers does not modify this existing CTR aggregation requirement, the beneficial ownership identification may provide banks with information they did not previously have, in order to determine when transactions are "by or on behalf of" the same person.

If a bank determines that a legal entity customer or customers are not being operated independently from each other or from their primary owner (the institution determines that legal entities under common ownership have common employees and are repeatedly used to pay each other's expenses or the personal expenses of their primary owner), then the bank may determine that aggregating the transactions of a legal entity or entities and their primary owner would be appropriate. Under such circumstances, if a bank were aware that a beneficial owner made a $5,000 cash deposit into his personal account, and later the same business day, he made a $6,000 cash deposit into the account of a legal entity not being operated as an independent entity, the institution would be required to aggregate those transactions and file a CTR. In addition, to the

extent that the bank determined that such transactions had no other apparent purpose than to avoid triggering a CTR filing, the bank would need to consider whether filing a SAR about the transactions would be appropriate.

FinCEN does not expect the information obtained pursuant to the beneficial ownership requirement to add additional requirements with respect to Section 314(a) for banks. The rule implementing Section 314(a), does not authorize the reporting of beneficial ownership information associated with an account or transaction matching a named subject. Under that rule, banks need only search their records for account or transactions matching a named subject, and report to FinCEN whether such a match exists using the identifying information that FinCEN provides.

Section 1010.230(c) Account.

There were no significant comments here. The definition of account did not change.

Section 1010.230(d) Beneficial Owner.

There are two prongs for the definition of beneficial owner: Each individual, if any, who directly or indirectly owned 25 percent of the equity interests of a legal entity customer (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 or any other individual who regularly performs similar functions (the control prong).

The number of beneficial owners identified would vary from legal entity customer to legal entity customer due to the ownership prong -there could be as few as zero and as many as four individuals who satisfy this prong. All legal entities, however, would be required to identify one beneficial owner under the control prong. Banks have the discretion to identify additional beneficial owners as appropriate based on risk.

Examples

Mr. and Mrs. Smith each hold a 50 percent equity interest in "Mom & Pop, LLC." Mrs. Smith is President of Mom & Pop, LLC and Mr. Smith is its Vice President. Mom & Pop, LLC is required to provide the personal information of both Mr. & Mrs. Smith under the ownership prong. Under the control prong, Mom & Pop, LLC is also required to provide the personal information of one individual with significant responsibility to control Mom & Pop, LLC; this individual could be either Mr. or Mrs. Smith, or a third person who otherwise satisfies the definition. Thus, in this scenario, Mom & Pop, LLC would be required to identify at least two, but up to three distinct individuals—both Mr. & Mrs. Smith under the ownership prong, and either Mr. or Mrs. Smith under the control prong, or both Mr. & Mrs. Smith under the ownership prong, and a third person with significant responsibility under the control prong.

Acme, Inc. is a closely held private corporation. John Roe holds a 35 percent equity stake; no other person holds a 25 percent or higher equity stake. Jane Doe is the President and Chief Executive Officer. Acme, Inc. would be required to provide John Roe's beneficial ownership information under the ownership prong, as well as Jane Doe's (or that of another control person) under the control prong.

Quentin, Inc. is owned by the five Quentin siblings, each of whom holds a 20 percent equity stake. Its President is Benton Quentin, the eldest sibling, who is the only individual at Quentin, Inc. with significant management responsibility. Quentin, Inc. would be required to provide

Benton Quentin's beneficial ownership information under the control prong, but no other beneficial ownership information under the ownership prong, because no sibling has a 25 percent stake or greater.

This obligation should be considered a snapshot, not a continuous obligation. FinCEN does expect banks to update this information based on risk, generally triggered by a bank learning through its normal monitoring of facts relevant to assessing the risk posed by the customer.

The Ownership Prong

The phrase "directly or indirectly," is intended to mean that the bank's customer identify its ultimate beneficial owner or owners as defined in the rule and not their nominees or "straw men." Banks may rely on information provided by the customer to identify and verify the beneficial owner.

The 25 percent threshold is the baseline regulatory benchmark, but banks may establish a lower percentage threshold for beneficial ownership (i.e., one that regards owners of less than 25 percent of equity interests as beneficial owners) based on their own assessment of risk in appropriate circumstances. FinCEN does not expect covered banks' compliance with this regulatory requirement to be assessed against a lower threshold.

FinCEN expects that banks will generally be able to rely on the representations of the customer when it identifies its beneficial owners. It would not be unreasonable to expect that a legal entity that has a complex structure would have personnel who necessarily have a general understanding of the ownership interests of the natural persons behind it for operational, management, accounting, and other purposes.

Exclusions in the rule include any entity organized under the laws of the United States or of any State, at least 51 percent of whose common stock or analogous equity interests are held by an entity listed on a U.S stock exchange. In the relatively unusual situations where an excluded entity holds a 25 percent or greater equity interest that is not covered by the exclusion, banks are not required under the ownership prong to identify and verify the identities of a natural person behind these entities; this is because the definition of "beneficial owner" under the ownership prong refers to "[e]ach individual, if any, . . .", and in such a case there would not be any individual who is the ultimate owner of such interest. On the other hand, where 25 percent or more of the equity interests of a legal entity customer are owned by a trust (other than a statutory trust), covered banks would satisfy the ownership prong of the beneficial ownership requirement by collecting and verifying the identity of the trustee, and FinCEN has amended the definition consistent with this approach.

The Control Prong

Legal entity customers are required to provide information on only one control person who satisfies the definition, so they should be able to readily identify at least one natural person within their management structure who has significant management responsibility. There may be legal entities for which there are no natural persons who satisfy the ownership prong; without the control prong, this would create a loophole for legal entities seeking to obscure their beneficial ownership information. Requiring the identification and verification of, at a minimum, one control person ensures that banks will have a record of at least one natural person associated with the legal entity, which will benefit all parties.

The control prong provides for a straightforward test: The legal entity customer must provide identifying information for one person with significant managerial control. It further provides as examples a number of common, well-understood senior job titles, such as President, Chief Executive Officer, and others. Taken together, these clauses provide ample information for legal entity customers to easily identify a natural person that satisfies the definition of control person.

The definition does not encapsulate all possible concepts of control, including effective control, however, the definition strikes a balance between including sufficiently senior leadership positions and practicability.

Section 1010.230(e) Legal Entity Customer

This paragraph defines the term "legal entity customer" and delineated a series of exclusions from this definition.

Section 1010.230(e)(1).

A legal entity customer means a corporation, limited liability company, or other entity that is 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.

This means that "legal entity customer" would include, in addition to corporations and limited liability companies, limited partnerships, business trusts that are created by a filing with a state office, any other entity created in this manner, and general partnerships. (It would also include similar entities formed under the laws of other countries.) It would not include sole proprietorships or unincorporated associations 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 an entity with legal existence separate from the associated individual or individuals that in effect creates a shield permitting an individual to obscure his or her identity. The definition of "legal entity customer" also does not include natural persons opening accounts on their own behalf.

Trusts

The definition would also not include trusts (other than statutory trusts created by a filing with a Secretary of State or similar office). Formation of a trust does not generally require any action by the state.

This does not and should not supersede existing obligations and practices regarding trusts generally. While banks 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." Moreover, where trusts are direct customers of banks, banks generally also identify and verify the identity of trustees, because trustees will necessarily be signatories on trust accounts (which in turn provides a ready source of information for law enforcement in the event of an investigation). 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." Consistent with existing obligations, banks are already taking a risk-based approach to collecting information with respect to various persons associated with trusts in order to know their customer, and that we expect banks to continue these practices.

"Account" Definition

A legal entity customer is defined as one that opens an account, as described in the CIP rules, which by its terms excludes an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

Section 1010.230(e)(2) Exclusions

All of the exclusions are a result of an assessment of the risks and determination that beneficial ownership information need not be obtained at account opening, because the information is generally available from other credible sources:

A bank regulated by a Federal functional regulator or a bank regulated by a State bank regulator - 1010.230(e)(2)(i)

These entities are excluded because they are subject to Federal or State regulation and information regarding their beneficial ownership and management is available from the relevant Federal or State agencies.

A person described in § 1020.315(b)(2) through (5) of this chapter -§ 1010.230(e)(2)(ii)

This includes the following:

- 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, of any State, or of any political subdivision of any State, or under an interstate compact between two or more States, that exercises governmental authority on behalf of the United States or of any such State or political subdivision.
- Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York, American, or NASDAQ stock exchange. This exclusion is appropriate because such entities are required to publicly disclose the beneficial owners of five percent or more of each class of the issuer's voting securities in periodic filings with the SEC, to the extent the information is known to the issuer or can be ascertained from public filings. In addition, beneficial owners of these issuers' securities may be subject to additional reporting requirements.
- Any entity organized under the laws of the United States or of any State at least 51 percent of whose common stock or analogous equity interests are held by a listed entity. Because such subsidiaries of listed entities are controlled by their parent listed entity, information regarding control and management is publicly available.

An issuer of a class of securities registered under section 12 of the Securities Exchange Act of 1934 or that is required to file reports under section 15(d) of that Act - § 1010.230(e)(2)(iii)

These issuers are excluded because they are required to publicly disclose the beneficial owners of five percent or more of each class of the issuer's voting securities in periodic filings with the SEC, to the extent the information is known to the issuer or can be ascertained from public filings. In addition, beneficial owners of the issuer's securities may be subject to additional reporting requirements.

An investment company, as defined in Section 3 of the Investment Company Act of 1940, that is registered with the SEC under that Act - § 1010.230(e)(2)(iv)

An investment adviser, as defined in section 202(a)(11) of the Investment Advisers Act of 1940, that is registered with the SEC under that Act -§ 1010.230(e)(2)(v)

These entities are excluded because registered investment companies and registered investment advisers already publicly report beneficial ownership in their filings with the SEC.

An exchange or clearing agency, as defined in section 3 of the Securities Exchange Act of 1934, that is registered under section 6 or 17A of that Act - § 1010.230(e)(2)(vi)

Any other entity registered with the SEC under the Securities and Exchange Act of 1934 - § 1010.230(e)(2)(vii)

These entities are excluded because the SEC registration process requires disclosure and regular updating of information about beneficial owners of those entities, as well as senior management and other control persons.

A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, each as defined in section 1a of the Commodity Exchange Act, that is registered with the CFTC - § 1010.230(e)(2)(viii)

These entities are excluded because the CFTC registration process requires disclosure and regular updating of information about beneficial owners of those entities, as well as senior management and other control persons.

A public accounting firm registered under section 102 of the Sarbanes-Oxley Act - § 1010.230(e)(2)(ix)

These firms are required to register with the Public Company Accounting Oversight Board (PCAOB), a nonprofit corporation established by Congress to oversee the audits of publicly traded companies, and are required to file annual and special reports with the PCAOB. In addition, States require public accounting firms to register and to file annual reports identifying their members (e.g., partners, members, or shareholders). Such information is often available online.

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)) - § 1010.230(e)(2)(x)

A pooled investment vehicle that is operated or advised by a bank excluded under this paragraph - § 1010.230(e)(2)(xi)

An insurance company that is regulated by a State - § 1010.230(e)(2)(xii)

For insurance companies regulated by a State of the United States, these companies must disclose and regularly update their beneficial owners, as well the identities of senior management and other control persons.

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 - § 1010.230(e)(2)(xiii)

FinCEN understands that entities designated as financial market utilities by the Financial Stability Oversight Council pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 are subject to extensive supervision and oversight by their Federal functional regulators, including the disclosure of beneficial ownership information. Accordingly, FinCEN believes that it is appropriate to exclude them from the definition.

Excluded Foreign Entities

A foreign bank established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution - § 1010.230(e)(2)(xiv)

With regard to regulated foreign banks, some commenters noted that in the rules implementing section 312 of the USA PATRIOT Act, even in the case of foreign banks subject to enhanced due diligence, a U.S. bank need obtain ownership information only if such foreign banks are not publicly traded, and that it would be inconsistent to impose a more burdensome requirement in the case of correspondent accounts for foreign banks (and arguably other foreign banks) that are not subject to enhanced due diligence. FinCEN agrees with this analysis and has broadened the exclusions to the definition of legal entity customer in the final rule to include foreign banks established in jurisdictions 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 - § 1010.230(e)(2)(xv)

Although the delineation between governmental and commercial activities arises out of well-recognized principles of sovereign immunity, FinCEN does not expect front-line employees of covered banks to engage in any type of legal analysis to determine the applicability of this exclusion. Rather, FinCEN expects covered banks to rely upon the representations of such customers, absent knowledge to the contrary.

Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620 - § 1010.230(e)(2)(xvi)

FinCEN's private banking account rule already requires banks maintaining such accounts to ascertain the identity of all beneficial owners of such accounts, but utilizes a different definition. Because covered banks have established a process for complying with the private banking account regulation, FinCEN has determined that it is appropriate to exclude such legal entity customers from the beneficial ownership requirement only when they establish such accounts.

Non-excluded Pooled Investment Vehicles

Because of the limited utility and difficulty of collecting beneficial ownership information under the ownership prong, in the case of pooled investment vehicles whose operators or advisers are not excluded from this definition, such as non-U.S. managed mutual funds, hedge funds, and private equity funds, banks would be required to collect beneficial ownership information under the control prong only.

Intermediated Account Relationships

In the NPRM it stated that if an intermediary is the customer, and the bank has no CIP obligation with respect to the intermediary's underlying clients pursuant to existing guidance, a bank should treat the intermediary, and not the intermediary's underlying clients, as its legal entity customer. Thus, existing guidance issued jointly by Treasury or FinCEN and any of the Federal functional regulators for broker-dealers, mutual funds, and the futures industry related to intermediated relationships would apply. FinCEN confirms that this principle will apply in interpreting the final rule, as follows: To the extent that existing guidance provides that, for purposes of the CIP rules, a bank shall treat an intermediary (and not the intermediary's customers) as its customer, the bank should treat the intermediary as its customer for purposes of this final rule. FinCEN also confirms that other guidance issued jointly by FinCEN and one or more Federal functional regulators relating to the application of the CIP rule will apply to this final rule, to the extent relevant.

Charities and Nonprofit Entities

In the NPRM, FinCEN proposed an exclusion from the definition of "legal entity customer" for charities and nonprofit entities that are described in sections 501(c), 527, or 4947(a)(1) of the Internal Revenue Code of 1986, which have not been denied tax exempt status, and which are required to and have filed the most recently due annual information return with the Internal Revenue Service.

Rather than limiting its treatment of this category to entities that are exempt from Federal tax and requiring proof of such exemption, FinCEN has determined that it would be simpler, as well as more efficient and more logical, to exclude all nonprofit entities (whether or not tax-exempt) from the ownership prong of the requirement, particularly considering the fact that nonprofit entities do not have ownership interests, and require only that they identify an individual with significant responsibility to control, manage, or direct the customer. The final rule includes as a type of legal entity customer, subject only to the control prong of the beneficial owner definition, any legal entity that is established as a nonprofit corporation or similar entity and has filed its organizational documents with the appropriate State authority as necessary.

A nonprofit corporation or similar entity would include, among others, charitable, nonprofit, not-for-profit, nonstock, public benefit or similar corporations. Such an organization could establish that it is a qualifying entity by providing a certified copy of its certificate of incorporation or a certificate of good standing from the appropriate State authority, which may already be required for a legal entity to open an account with a bank under its CIP. Small local community organizations, such as Scout Troops and youth sports leagues, are unincorporated associations rather than legal entities and therefore not subject to the beneficial ownership requirement.

Section 1010.230(f) Covered Bank

This paragraph defines covered bank by reference to the definition set forth in § 1010.605(e)(1), thereby subjecting to this requirement those banks already covered by CIP requirements.

Section 1010.230(g) New account

See discussion above under "Identification and Verification."

Section 1010.230(h) Exemptions

This paragraph exempts covered banks from the beneficial ownership requirement with respect to opening accounts for legal entity customers for certain specific activities and within certain limitations for the reasons described below.

Private Label Retail Credit Accounts Established at the Point-of-Sale

Covered banks are exempt from the beneficial ownership requirement with respect to private label credit card accounts to the limited extent that they are established at the point-of-sale to obtain credit products, including commercial private label credit cards, solely for the purchase of retail goods and/or services at the issuing retailer and have a credit limit of no more than $50,000.

In contrast, credit cards that are co-branded with major credit card associations do not possess the same limitations and characteristics that would protect them from abuse. For example, co-branded credit cards can be used at any outlet or ATM that accepts those associations' cards. FinCEN therefore believes that covered banks should obtain and verify beneficial ownership information with respect to opening accounts for legal entities involving such co-branded cards.

Accounts Established for the Purchase and Financing of Postage

Covered banks are exempt from the beneficial ownership requirement with respect to accounts solely used to finance the purchase of postage and for which payments are remitted directly by the bank to the provider of the postage products.

Commercial Accounts to Finance Insurance Premiums

Covered banks are exempt from the beneficial ownership requirement with respect to accounts solely used to finance insurance premiums and for which payments are remitted directly by the bank to the insurance provider or broker.

Accounts To Finance the Purchase or Lease of Equipment

Covered banks are exempt from the beneficial ownership requirement with respect to accounts solely used to finance the purchase or leasing of equipment and for which payments are remitted directly by the bank to the vendor or lessor of this equipment.

Section 1010.230(h)(2) Limitations on Exemptions

These three exemptions are subject to further limitations to mitigate the remaining limited money laundering risks associated with them, as follows:

- The exemptions identified in paragraphs (h)(1)(ii) through (iv) do not apply to transaction accounts through which a legal entity customer can make payments to, or receive payments from, third parties.
- If there is the possibility of a cash refund on the account activity identified in paragraphs (h)(1)(ii) through (iv), then beneficial ownership of the legal entity customer must be identified and verified by the bank as required by this section, either at the time of initial remittance, or at the time such refund occurs.

Section 1010.230(i) Recordkeeping.

Under the proposal, a bank must have procedures for maintaining a record of all information obtained in connection with identifying and verifying beneficial owners, including retention of the Certification Form and a record of any other related identifying information reviewed or collected, for a period of five years after the date the account is closed. Furthermore, a bank must also retain records for a period of five years after such record is made, including 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 verifying the identification information.

Because collection of the Certification Form is no longer a requirement, there was a corresponding change to the recordkeeping requirement for the final rule. Section 1010.230(i)(1)(i) now states that at a minimum, the record must include, for identification, any identifying information obtained by the covered bank pursuant to paragraph (b), including without limitation the certification (if obtained).

Section 1010.230(j) Reliance on Another Bank.

In the NPRM, banks could rely on the performance by another bank of the requirements of this section under the same conditions as set forth in the applicable CIP rules. The final rule maintains this position. Section 1020.210 Anti-money laundering program requirements for banks regulated only by a Federal functional regulator, including banks, savings associations, and credit unions.

FinCEN proposed to amend its existing AML program rules to expressly incorporate both the minimum statutory elements of an AML program prescribed by 31 U.S.C. 5318(h)(1), as well as the elements of the minimum standard of CDD that are not otherwise already accounted for in either the existing AML regulatory scheme (i.e., CIP) or in the proposed beneficial ownership requirement.

Paragraphs (b)(1) through (4) correspond to the minimum statutory elements of section 5318(h)(1), while proposed paragraph (b)(5) set forth the remaining elements of CDD by requiring appropriate risk-based procedures for conducting ongoing customer due diligence including, but not limited to

- understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and
- conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions.

These elements of CDD were necessary and critical steps required to comply with the existing requirement under the BSA to identify and report suspicious transactions. Thus, expressly incorporating them into the AML program rules would serve to harmonize these elements with existing AML obligations.

Under the existing requirement for banks to report suspicious activity, they must file SARs on a transaction that, among other things, has "no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage." Banks specifically are expected to "obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations." In short, to understand the types of transactions in which a particular customer would normally be expected to engage necessarily requires an understanding of the nature and purpose of the customer relationship, which informs the baseline against which aberrant, suspicious transactions are identified. In some circumstances an understanding of the nature and purpose of a customer relationship can also be developed by inherent or self-evident information about the product or customer type, such as the type of customer, the type of account opened, or the service or product offered, or other basic information about the customer, and such information may be sufficient to understand the nature and purpose of the relationship. Depending on the facts and circumstances, other relevant facts could include basic information about the customer, such as annual income, net worth, domicile, or principal occupation or business, as well as, in the case of longstanding customers, the customer's history of activity.

Conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions is consistent with current industry practice. Banks are expected to have in place internal controls to "provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity."

FinCEN views this "fifth pillar" as nothing more than an explicit codification of existing expectations; as these expectations should already be taken into account in a bank's internal controls, FinCEN would expect the confusion caused by this codification, if any, to be minimal. In order to bring uniformity and consistency across sectors, it is important that these due diligence elements be made explicit, and that they be part of the AML program of depository institutions (as well as of the other covered banks).

For banks, the term "customer risk profile" is used to refer to the information gathered about a customer to develop the baseline against which customer activity is assessed for suspicious transaction reporting. As such, we would not expect there to be any significant changes to current practice that is consistent with existing expectations and requirements, and certainly not in the form of inappropriate profiling.

The final rule amends the ongoing monitoring prong to state that ongoing monitoring is conducted to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. For these purposes, customer information shall include information regarding the beneficial owners of legal entity customers (as defined in § 1010.230).

When banks become aware of new information during the course of their normal monitoring relevant to assessing or reevaluating the risk of a customer relationship, for instance 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 event, it is appropriate to update the customer information accordingly. Including the ongoing monitoring element in the AML program rules serves to reflect existing practices to satisfy SAR reporting obligations. Although the beneficial ownership information collection requirement was not in place at the time of the proposal, this information may be relevant in assessing the risk posed by the customer and in assessing whether a transaction is suspicious.

FinCEN believes it is also consistent that this updating requirement should apply not only to customers with new accounts, but also to customers with accounts existing on the Applicability Date. That is, should the bank learn as a result of its normal monitoring that the beneficial owner of a legal entity customer may have changed, it should identify the beneficial owner of such customer. For example, envision a situation where an unexpected transfer of all of the funds in a legal entity's account to a previously unknown individual would trigger an investigation in which the bank learns that the funds transfer was directly related to a change in the beneficial ownership of the legal entity. The obligation to update customer information pursuant to this provision, including beneficial ownership information, is triggered only when, in the course of its normal monitoring, the bank detects information relevant to assessing the risk posed by the customer; it is not intended to impose a categorical requirement to update customer or beneficial ownership information on a continuous or ongoing basis.

FinCEN believes that the revision of the ongoing monitoring element for the final rule as the requirement is consistent with current practice, and monitoring-triggered updating of beneficial ownership information (as with other customer information) should only occur on a risk basis when material information about a change in beneficial ownership is uncovered during the course of a bank's normal monitoring (whether of the customer relationship or of transactions). There may be unusual cases where transaction monitoring might lead to information about a possible change in beneficial ownership. However, there is no expectation that a bank obtain updated beneficial ownership information from its customers on a regular basis, whether by using the Certification Form in Appendix A or by any other means.

Section 1023.210 Anti-money laundering program requirements for brokers or dealers in securities.

Section 1024.210 Anti-money laundering program requirements for mutual funds.

Section 1026.210 Anti-money laundering program requirements for futures commission merchants and introducing brokers in commodities.

As these sections do not apply to the attendees, they have been omitted.