

Customer Due Diligence — Overview

Objective. *Assess the bank’s compliance with the regulatory requirements for customer due diligence (CDD).*

The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of risk-based CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD is to enable the bank to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious.

Effective CDD policies, procedures, and processes provide the critical framework that enables the bank to comply with regulatory requirements including monitoring for and reporting of 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 activity that potentially exposes the bank to financial loss, increased expenses, or other risks.
- 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.

Customer Due Diligence

FinCEN’s final rule on CDD became effective July 11, 2016, with a compliance date of May 11, 2018. The rule codifies existing supervisory expectations and practices related to regulatory requirements and therefore, nothing in this final rule is intended to lower, reduce, or limit the due diligence expectations of the federal functional regulators or in any way limit their existing regulatory discretion.¹

In accordance with regulatory requirements, all banks must develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence,² including, but not limited to:

- Obtaining and analyzing sufficient customer information to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information

¹ Department of the Treasury, Financial Crimes Enforcement Network (2016), “Customer Due Diligence Requirements for Financial Institutions,” final rules (RIN 1506-AB25), *Federal Register*, vol. 81 (May 11), p. 29403.

² See 31 CFR 1020.210(b)(5)

regarding the beneficial owner(s) of legal entity customers. Additional guidance can be found in the examination procedures “Beneficial Ownership Requirements for Legal Entity Customers.”

At a minimum, the bank must establish risk-based CDD procedures that:

- Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
- Enable the bank to conduct ongoing monitoring
 - for the purpose of identifying and reporting suspicious transactions and,
 - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.

In addition, the bank’s risk-based CDD policies, procedures, and processes should:

- Be commensurate with the bank’s BSA/AML risk profile, with increased focus on higher risk customers.
- Contain a clear statement of management’s and staff’s responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer’s risk profile, as applicable.
- Provide standards for conducting and documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

Customer Risk Profile

The bank should have an understanding of the money laundering and terrorist financing risks of its customers, referred to in the rule as the customer risk profile.³ This concept is also commonly referred to as the customer risk rating. Any customer account may be used for illicit purposes, including money laundering or terrorist financing. Further, a spectrum of risks may be identifiable even within the same category of customers. The bank’s program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the money laundering and terrorist financing risks of its customers. Improper identification and assessment of a customer’s risk can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened BSA compliance program.

The assessment of customer risk factors is bank-specific, and a conclusion regarding the customer risk profile should be based on a consideration of all pertinent customer information, including ownership information generally. Similar to the bank’s overall risk assessment, there are no required risk profile categories and the number and detail of these categorizations will vary based on the bank’s size and complexity. Any one single indicator is not necessarily determinative of the existence of a lower or higher customer risk.

³See 31 CFR 1020.210(b)(5)(i)

Examiners should primarily focus on whether the bank has effective processes to develop customer risk profiles as part of the overall CDD program. Examiners may review individual customer risk decisions as a means to test the effectiveness of the process and CDD program. In those instances where the bank has an established and effective customer risk decision-making process, and has followed existing policies, procedures, and processes, the bank should not be criticized for individual customer risk decisions unless it impacts the effectiveness of the overall CDD program, or is accompanied by evidence of bad faith or other aggravating factors.

The bank should gather sufficient information about the customer to form an understanding of the nature and purpose of customer relationships at the time of account opening. This understanding may be based on assessments of individual customers or on categories of customers. An understanding based on “categories of customers” means that for certain lower-risk customers, the bank’s understanding of the nature and purpose of a customer relationship can be developed by inherent or self-evident information such as the type of customer, the type of account opened, or the service or product offered.

The factors the bank should consider when assessing a customer risk profile are substantially similar to the risk categories considered when determining the bank’s overall risk profile. The bank should identify the specific risks of the customer or category of customers, and then conduct an analysis of all pertinent information in order to develop the customer’s risk profile. In determining a customer’s risk profile, the bank should consider risk categories, such as the following, as they relate to the customer relationship:

- Products and Services.
- Customers and Entities.
- Geographic Locations.

As with the risk assessment, the bank may determine that some factors should be weighted more heavily than others. For example, certain products and services used by the customer, the type of customer’s business, or the geographic location where the customer does business, may pose a higher risk of money laundering or terrorist financing. Also, actual or anticipated activity in a customer’s account can be a key factor in determining the customer risk profile. Refer to the further description of identification and analysis of specific risk categories in the “BSA/AML Risk Assessment - Overview” section of the FFIEC BSA/AML Examination Manual.

Customer Information – Risk-Based Procedures

As described above, the bank is required to form an understanding of the nature and purpose of the customer relationship. The bank may demonstrate its understanding of the customer relationship through gathering and analyzing information that substantiates the nature and purpose of the account. Customer information collected under CDD requirements for the purpose of developing a customer risk profile and ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, includes beneficial ownership information for legal entity customers. However, the collection of customer information regarding beneficial ownership is governed by the

requirements specified in the beneficial ownership rule. The beneficial ownership rule requires the bank to collect beneficial ownership information at the 25 percent ownership threshold regardless of the customer's risk profile. In addition, the beneficial ownership rule does not require the bank to collect information regarding ownership or control for certain customers that are exempted or not included in the definition of legal entity customer, such as certain trusts, or certain other legal entity customers.⁴

Other than required beneficial ownership information, the level and type of customer information should be commensurate with the customer's risk profile, therefore the bank should obtain more customer information for those customers that have a higher customer risk profile and may find that less information for customers with a lower customer risk profile is sufficient. Additionally, the type of appropriate customer information will generally vary depending on the customer risk profile and other factors, for example, whether the customer is a legal entity or an individual. For lower risk customers, the bank may have an inherent understanding of the nature and purpose of the customer relationship (*i.e.*, the customer risk profile) based upon information collected at account opening. As a result, the bank may not need to collect any additional customer information for these customers in order to comply with this part of the CDD requirements.

Customer information collected under the CDD rule may be relevant to other regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties. The bank should define in its policies, procedures and processes how customer information will be used to meet other regulatory requirements. For example, the bank is expected to use the customer information and customer risk profile in its suspicious activity monitoring process to understand the types of transactions a particular customer would normally be expected to engage in as a baseline against which suspicious transactions are identified and to satisfy other regulatory requirements.⁵

The bank may choose to implement CDD policies, procedures, and processes on an enterprise-wide basis. To the extent permitted by law, this implementation may include sharing or obtaining customer information across business lines, separate legal entities within an enterprise, and affiliated support units. To encourage cost effectiveness, enhance efficiency, and increase availability of potentially relevant information, the bank may find it useful to cross-check for customer information in data systems maintained within the financial institution for other purposes, such as credit underwriting, marketing, or fraud detection.

Higher Risk Profile Customers

Customers that pose higher money laundering or terrorist financing risks, (*i.e.*, higher risk profile customers), present increased risk exposure to banks. As a result, due diligence policies, procedures, and processes should define both when and what additional customer information will be collected based on the customer risk profile and the specific risks posed. Collecting additional information about customers that pose heightened risk, referred to as enhanced due diligence (EDD), for example, in the private and foreign correspondent banking context, is part

⁴ See 31 CFR 1010.230(e)(2) and 31 CFR 1010.230(h)

⁵ See 31 CFR 1020.210(b)(5)(ii)

of an effective due diligence program. Even within categories of customers with a higher risk profile, there can be a spectrum of risks and the extent to which additional ongoing due diligence measures are necessary may vary on a case-by-case basis. Based on the customer risk profile, the bank may consider obtaining, at account opening (and throughout the relationship), more customer information in order to understand the nature and purpose of the customer relationship, such as:

- Source of funds and wealth.
- Occupation or type of business (of customer or other individuals with ownership or control over the account).
- Financial statements for business customers.
- Location where the business customer is organized and where they maintain their principal place of business.
- Proximity of the customer's residence, place of employment, or place of business to the bank.
- Description of the business customer's primary trade area, whether transactions are expected to be domestic or international, and the expected volumes of such transactions.
- Description of the business operations, such as total sales, the volume of currency transactions, and information about major customers and suppliers.

Performing an appropriate level of ongoing due diligence that is commensurate with the customer's risk profile is especially critical in understanding the customer's transactions in order to assist the bank in determining when transactions are potentially suspicious. This determination is necessary for a suspicious activity monitoring system that helps to mitigate the bank's compliance and money laundering risks.

Consistent with the risk-based approach, the bank should do more in circumstances of heightened risk, as well as to mitigate risks generally. Information provided by higher risk profile customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank. The bank should establish policies and procedures for determining whether and/or when, on the basis of risk, obtaining and reviewing additional customer information, for example through negative media search programs, would be appropriate.

While not inclusive, certain customer types, such as those found in the "Persons and Entities" section of the FFIEC BSA/AML Examination Manual, may pose heightened risk. In addition, existing laws and regulations may impose, and supervisory guidance may explain expectations for, specific customer due diligence and, in some cases, enhanced due diligence requirements for certain accounts or customers, including foreign correspondent accounts,⁶ payable-through

⁶ See 31 CFR 1010.610.

accounts,⁷ private banking accounts,⁸ politically exposed persons,⁹ and money services businesses.¹⁰ The bank's risk-based customer due diligence and enhanced due diligence procedures must ensure compliance with these existing requirements and should meet these supervisory expectations.

Ongoing Monitoring of the Customer Relationship

The requirement for ongoing monitoring of the customer relationship reflects existing practices established to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

Therefore, in addition to policies, procedures, and processes for monitoring to identify and report suspicious transactions, the bank's CDD program must include risk-based procedures for performing ongoing monitoring of the customer relationship, on a risk basis, to maintain and update customer information, including beneficial ownership information of legal entity customers.¹¹ For more information on beneficial ownership of legal entity customers, refer to the "Beneficial Ownership Requirements for Legal Entity Customers" section of the FFIEC BSA/AML Examination Manual.

The requirement to update customer information is event-driven and occurs as a result of normal monitoring.¹² Should the bank become aware as a result of its ongoing monitoring that customer information, including beneficial ownership information, has materially changed, it should update the customer information accordingly. Additionally, if this customer information is material and relevant to assessing the risk of a customer relationship, then the bank should reassess the customer risk profile/rating and follow established bank policies, procedures, and processes for maintaining or changing the customer risk profile/rating. One common indication of a material change in the customer risk profile is transactions or other activity that are inconsistent with the bank's understanding of the nature and purpose of the customer relationship or with the customer risk profile.

The bank's procedures should establish criteria for when and by whom customer relationships will be reviewed, including updating customer information and reassessing the customer's risk profile. The procedures should indicate who in the organization is authorized to change a customer's risk profile. A number of factors may be relevant in determining when it is appropriate to review a customer relationship including, but not limited to:

- Significant and unexplained changes in account activity
- Changes in employment or business operation

⁷ See 31 CFR 1010.610(b)(1)(iii).

⁸ See 31 CFR 1010.620

⁹ Department of State, Department of the Treasury, Federal Reserve, FDIC, OCC, OTS, *Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds of Official Corruption*, January 1, 2001.

¹⁰ FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States*, April 26, 2005.

¹¹ See 31 CFR 1020.210(b)(5)(ii)

¹² Department of the Treasury, Financial Crimes Enforcement Network (2016), "Customer Due Diligence Requirements for Financial Institutions," final rules (RIN 1506-AB25), *Federal Register*, vol. 81 (May 11), p. 29399.

- Changes in ownership of a business entity
- Red flags identified through suspicious activity monitoring
- Receipt of law enforcement inquiries and requests such as criminal subpoenas, National Security Letters (NSL), and section 314(a) requests
- Results of negative media search programs
- Length of time since customer information was gathered and the customer risk profile assessed

The ongoing monitoring element does not impose a categorical requirement that the bank must update customer information on a continuous or periodic basis.¹³ However, the bank may establish policies, procedures, and processes for determining whether and when, on the basis of risk, periodic reviews to update customer information should be conducted to ensure that customer information is current and accurate.

¹³ Ibid.

Examination Procedures

Customer Due Diligence

Objective. *Assess the bank's compliance with the regulatory requirements for customer due diligence (CDD).*

1. Determine whether the bank has developed and implemented appropriate written risk-based procedures for conducting ongoing CDD and that they:
 - Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
 - Enable the bank to conduct ongoing monitoring
 - for the purpose of identifying and reporting suspicious transactions and,
 - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.
 - Enable the bank to use customer information and the customer risk profile to understand the types of transactions a particular customer would be expected to engage in and as a baseline against which suspicious transactions are identified.
2. Determine whether the bank, as part of the overall CDD program, has effective processes to develop customer risk profiles that identify the specific risks of individual customers or categories of customers.
3. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the bank's BSA/AML risk profile with increased focus on higher risk customers.
4. Determine whether policies, procedures, and processes contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable.
5. Determine that the bank has policies, procedures, and processes to identify customers that may pose higher risk for money laundering or terrorist financing that include whether and/or when, on the basis of risk, it is appropriate to obtain and review additional customer information.
6. Determine whether the bank provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.
7. Determine whether the bank has defined in its policies, procedures, and processes how customer information, including beneficial ownership information for legal entity customers, is used to meet other relevant regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties.

Transaction Testing

8. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of customer information. Determine whether the bank collects appropriate information sufficient to understand the nature and purpose of the customer relationship and effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. This sample can be performed when testing the bank's compliance with its policies, procedures, and processes as well as when reviewing transactions or accounts for possible suspicious activity.
9. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with CDD.