



FinCEN GUIDANCE

FIN-2020-G002

Issued: August 3, 2020

Subject: Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions.

The Financial Crimes Enforcement Network (FinCEN), in consultation with the federal functional regulators, is issuing responses to three frequently asked questions (FAQs) regarding customer due diligence requirements for covered financial institutions. These FAQs clarify the regulatory requirements related to obtaining customer information, establishing a customer risk profile, and performing ongoing monitoring of the customer relationship in order to assist covered financial institutions with their compliance obligations in these areas. These FAQs are in addition to those that were published on [July 19, 2016](#) and [April 3, 2018](#). For further information regarding customer due diligence requirements, including the Customer Due Diligence Requirements for Financial Institutions¹ (the “CDD Rule”), please see FinCEN’s [CDD webpage](#).

I. Customer Information – Risk-Based Procedures

Q1: Is it a requirement under the CDD Rule that covered financial institutions:

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

1. See 31 U.S.C § 5318(h) and 31 CFR § 1010.210 for anti-money laundering program requirements, and, as applied to specific financial institutions, in 31 CFR §§ 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, and 1030.210.

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

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

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

II. Customer Risk Profile

Q2: Is it a requirement under the CDD Rule that covered financial institutions:

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

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

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

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

III. Ongoing Monitoring of the Customer Relationship

Q3: *Is it a requirement under the CDD Rule that financial institutions update customer information on a specific schedule?*

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

For Further Information

Questions or comments regarding the contents of this guidance should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.