Customer Due Diligence (CDD) &
Anti-money Laundering (AML) Controls
Brandi Reynolds, CAMS-Audit

"Knowing Your Customer" is critical for any financial institution. To adequately Know Your Customer ("KYC"), a financial institution must conduct proper Customer Due Diligence (CDD). Financial institutions are often scrutinized by regulators for having weak or inadequate controls in this area. Specifically, Regulators are concerned with the lack of uniformity and consistency with CDD compliance. Lack of effective controls may render a financial institution's AML Program inadequate.

Beginning on May 11, 2018, covered financial institutions must comply with new FinCEN rules that were finalized on July 11, 2016.[1] "Covered financial institutions" are those that are already subject to Bank Secrecy Act (BSA) Customer Identification Program (CIP) requirements such as: depository institutions, mutual funds, securities brokers, and futures commission merchants and, introducing brokers in commodities. These rules are best practices for other financial institutions as well as non-financial institutions that partner with banks.

What are the core elements of CDD?

FinCEN indicates that there are four core elements of CDD and should be explicit requirements in the anti-money laundering (AML) program for all required financial institutions. Requiring a covered financial institution to incorporate these elements into its AML Program will allow for clarity and consistency across sectors.[2] The four core CDD elements are:

1. Customer identification and verification- CDD begins with verifying the customer's identity. Financial institutions must identify and verify customers on a risk-based approach to ensure there's a reasonable belief as to the true identity of the customer.[3]

2. Beneficial ownership identification and verification- Financial institutions shall identify beneficial owners of all customers and verify their identities using a risk-based approach.

3. Understanding the nature and purpose of customer relationships to develop a customer risk profile- Regulated financial institutions should understand the nature and purpose of the transaction as well as expected activity. This will assist in assessing the risk and identifying and reporting suspicious activity.

4. Ongoing CDD- Financial institutions shall establish policies and procedures for conducing ongoing monitoring of all customers/transactions for reporting suspicious transactions and, on a risk-basis, maintain and update customer information.

How can financial institutions mitigate their risk?

Financial institutions can mitigate their risk of non-compliance by creating and maintaining a client risk profile. Financial institutions should maintain a process for identifying and managing high-risk customers and transactions that includes procedures for enhanced due diligence (EDD).

[1] https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf
[2] https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf
[3] https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm) and
https://www.ecfr.gov/cgi-bin/text-idx?SID=9bd185e43e8c6b2ef75acbb2e228806d&mc=true&node=se31.3.1022_1210&rgn=div8

The dilemma that financial institutions have is that there is not a "one size fits all" approach to complying with the CDD requirements. Therefore, financial institutions must employ a risk-based approach.

To determine the relevant risks, financial institutions must obtain information, similar to the information listed below, to determine the following:

- Purpose of the transaction or business relationship;
- Expected pattern of activity (e.g. volume and transaction amounts)
- Origination and destination of funds (if applicable)
- Beneficial owners;
- Geographic location of the customer.

What you should know about high-risk accounts…

It is likely that high-risk accounts may be identified during the CDD process. It is important that EDD is conducted on all high-risk customers/transactions and properly documented, because these are often scrutinized by regulators. Below are some things you should know about high-risk accounts.

- Regulators often scrutinize high-risk accounts and the process to identify them.
- Politically Exposed Persons (PEPs) may be considered high-risk customers.
- Risk ratings must adequately rate the risk of the customers and be linked to the process for monitoring and reporting suspicious activity.
- Enhanced monitoring is required for high-risk customers/transactions.

AML Controls for compliance

Failure to implement adequate internal controls is frequently cited in enforcement actions issued by FinCEN[4]. Regulators often rely on independent annual testing as reassurance that AML program requirements are being followed by the financial institution. This testing includes verification of adequate controls such as policies and procedures and transaction testing. However, it is no longer sufficient that these controls are in place. Regulators now want assurance that the financial institution is effectively implementing these controls.

What Controls do you need?

No matter the type and size of your financial institution, there are certain standard controls that should be considered to assist you in your compliance efforts with CDD requirements.

[4] https://www.fincen.gov/news-room/enforcement-actions

- Suspicious Activity Monitoring- Are there adequate technical and/or human resources for detecting suspicious activity?
- Policies and Procedures- The AML Compliance Program should be supplemented with policies and procedures. These should be regularly updated.
- Customer Risk Rating- The risk rating approach/methodology should be updated regularly to consider changes in products and services offered.

Conclusion

The cornerstone of a strong BSA/AML compliance program rests in the adoption and implementation of comprehensive CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. An effective BSA/AML Compliance Program must incorporate CDD, EDD, and proper AML Controls to meet regulator's scrutiny.