ACAMS® | Advancing Financial Crime Professionals Worldwide

Benefits of an Effective CDD Program and How Risk Scoring Customer Accounts Can Protect the Reputation of Your Institution

By: Douglas J. Bruggeman

Contents

Statement of Intent:

The following white paper, *Benefits of an Effective CDD Program and How Risk Scoring Customer Accounts Can Protect the Reputation of Your Institution*, is intended to show the importance of a formal customer due diligence (CDD) program and how it must be designed to conform to current securities industry regulations pertaining to policies, procedures and processes. In addition to discussing a formal CDD program, this white paper will also discuss risk scoring a customer, including general risk scoring policies, procedures and processes.

Specifically, this paper will provide important guidance and information on how you can protect the reputation of securities firms and other financial institutions through discussions on the following topics: The history of CDD programs and risk scoring customers; the benefits of effective CDD programs and risk scoring customers; how CDD programs and risk scoring works, including examples of effective CDD programs and risk scoring methods; problems associated with CDD programs and risk scoring customers; what and where to look for when considering solutions; and specific solutions and what actions your financial firm should consider implementing.

Various resources have been relied on for this white paper to provide specific and recent information pertaining to CDD programs and risk scoring customers; Bank Secrecy Act/anti-money laundering (BSA/AML) industry regulations, policies, procedures and processes. For further information see the bibliography at the end of this document.

"Customer Due Diligence (CDD)"

While CDD is not explicitly required under U.S. regulations, regulatory guidance recommends that all securities firms and financial institutions have policies, procedures and processes in place that include CDD procedures to know each customer and understand the reputational risks that the customer may pose to a financial institution. A securities firm's basis of a CDD program should be made up of four traditional elements:

- Customer Identification Program (CIP)
- Initial due diligence,
- Ongoing monitoring and enhanced due diligence
- Reporting and escalation

On July 30, 2014, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)[1] issued a proposed regulation that would formalize certain requirements for how certain financial institutions conduct CDD. The proposed regulation adds a CDD requirement as a fifth pillar to the traditional four-pillar AML program requirement.

Customer Due Diligence

Many experts say that "a CDD program is the best way to prevent money laundering. Knowledge is what the entire anti-money laundering (AML) compliance program is built on. The more you and your institution know, the better money laundering abuses can be prevented."[2]

In addition to the four basic elements listed above, a sound CDD program should include these seven additional elements:

- "Full identification of customer and business entities, including source of funds and wealth when appropriate
- Development of transaction and activity profiles of each customer's anticipated activity
- Definition and acceptance of the customer in the context of specific products and services
- Assessment and grading of risks that the customer or the account presents
- Account and transaction monitoring based on the risks presented
- Investigation and examination of unusual customer or account activity
- Documentation of findings"[3]

An effective CDD program will provide securities firms and financial institutions the ability to gauge the risk presented by each customer and entity by providing the firm with a reference point for evaluating customer transactions to determine whether the transactions are suspicious and need to be reported.

[1] https://www.fincen.gov/statutes_regs/files/CDD-NPRM-Final.pdf
[2] http://files.acams.org/pdfs/English_Study_Guide/Chapter_4.pdf
[3] Ibid.

Most securities firms and financial institutions recognize that having a strong CDD program that goes beyond the standard CIP requirements is the basis of a solid AML compliance program.

Many securities firms and financial institutions follow guidelines found in the *FFIEC BSA/AML Customer Due Diligence Overview* online manual. Relevant excerpts are discussed below.

CDD Guidance

BSA/AML policies, procedures and processes should include CDD guidelines that:

- "Are commensurate with the bank's BSA/AML risk profile, paying particular attention to higher risk customers;
- Contain a clear statement of management's overall expectations and establish specific staff responsibilities, including who is responsible for reviewing or approving changes to a customer's risk rating or profile, as applicable;
- Ensure that the bank possesses sufficient customer information to implement an effective suspicious activity monitoring system;
- Provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained; and
- Ensure the bank maintains current customer information." [4]

Securities firms are required by federal law to obtain and verify certain identification information from all customers as defined by the U.S. Department of the Treasury, Securities and Exchange Commission, and FINRA rules. This is commonly referred to as the CIP.

The following is an excerpt from FINRA's *Customer Identification Program Notice: Important Information You Need to Know about Opening a New Account*:[5]

"To help the government fight the funding of terrorism and money laundering activities, federal law requires financial institutions to obtain, verify and record information that identifies each person who opens an account.

This notice answers some questions about your firm's CIP.

What types of information will I need to provide?

When you open an account, your firm is required to collect the following information:

- Name
- Date of birth
- Address
- Identification number
- U.S. citizen: taxpayer identification number (Social Security number or employer identification number)

[4] https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_013.htm
[5] http://www.finra.org/industry/customer-identification-program-notice

- Non-U.S. citizen: taxpayer identification number; passport number and country of issuance; alien identification card number; or government-issued identification showing nationality, residence and a photograph of you.

You may also need to show your driver's license or other identifying documents.

A corporation, partnership, trust or other legal entity may need to provide other information, such as its principal place of business, local office, employer identification number, certified articles of incorporation, government-issued business license, a partnership agreement or a trust agreement.

The U.S. Department of the Treasury, Securities and Exchange Commission and FINRA rules already require you to provide most of this information. These rules also may require you to provide additional information, such as your net worth, annual income, occupation, employment information, investment experience and objectives and risk tolerance.

What happens if I do not provide the information requested or my identity can't be verified?

Your firm may not be able to open an account or carry out transactions for you. If your firm has already opened an account for you, they may have to close it."

As defined by the **American Bankers Association/ABA Banking Journal**, In January 2016, the ABA sent a letter to the director of the Financial Crimes Enforcement Network (FinCEN) questioning the cost-benefit analysis of FinCEN's new proposed CDD rule.[6]The proposed rule (a) would require financial institutions to identify the beneficial owners of a legal entity who hold a 25 percent or greater ownership, including the individual who controls the entity. The ABA questions FinCEN's undertaking of the CDD rule cost-benefit analysis, where a very limited number banks and only three small institutions were included in FinCEN's sampling. The ABA expressed concerns that FinCEN failed to access accurate costs that would be required by a financial institutions for the staffing hours, training of employees and upgrading systems needed to be compliant with the proposed rule.

(a) FinCEN 31 CFR 1010, 1020,1023,1024 and 1026, RIN 1506-AB25, Customer Due Diligence Requirements for Financial Institutions

Many of the large securities firms and financial institutions are struggling with the costs and staffing problems associated with newly proposed CDD programs and risk scoring customers rules.

The following is an excerpt from the *ABA Journal*:

ABA Challenges Cost-Benefit Analysis of Customer Due Diligence Proposal
January 28, 2016

In a comment letter yesterday, ABA criticized the Financial Crimes Enforcement Network's recent cost-benefit analysis of its proposed customer due diligence rule, claiming that the analysis relies on unsubstantiated and overly optimistic assumptions about the potential benefits of the heightened requirements and fails to adequately identify and weigh the burden imposed on financial institutions.

[6] "Notice of Availability of Regulatory Impact Assessment and Initial Regulatory Flexibility Analysis Regarding the Customer Due Diligence Requirements for Financial Institutions, 80 Fed. Reg. 80308 (Dec. 24, 2015)."

The proposed rule would require banks to identify the beneficial owners of legal entity customers who hold a 25 percent or greater ownership stake in the legal entity, as well as the individual who controls the entity.

ABA pointed out that FinCEN's analysis of the rule — which sampled only a small handful of banks and just three small institutions — failed to accurately assess the costs banks would incur for the staff time, training and system upgrades needed to come into compliance. Nor, the letter added, did it address the potential effects of derisking that could occur as banks face pressure to satisfy new regulatory requirements. ABA urged FinCEN not to proceed with a final rule until a proper cost-benefit analysis has been completed.[7]

"Risk Scoring"

The securities and financial institutions industry rules and regulations have many specific guidelines pertaining to BSA/AML Risk Profile and Risk Assessment. However, the industry rules and regulations are not very clear when it comes to specific guidelines and requirements defining how or when securities and financial institutions are required to assign a risk score to a customer or entity. Many securities and financial institutions are learning the benefits of risk scoring to identify the level of risk associated with a new customer or account by efficiently capturing CDD information during onboarding and ongoing monitoring. The use of due diligence information can generate an initial score for each new customer/account and ongoing transaction data from existing monitoring systems (particularly high risk transaction activity) to build and continuously update the customers risk score within a "Risk Profile" for each customer or entity.

The following is an excerpt from the ACAMS English CAMS Study Guide:

Assessing Risk and Developing a Risk-Scoring Model

Understanding what is legally required of your institution, employees and customers is essential to a successful program.

Whatever those legal requirements, however, FATF, along with numerous member countries, such as the United Kingdom and United States, urge risk-based controls.

The theory is that no financial institution can reasonably be expected to detect all wrongdoing by customers, including money laundering. But if an institution develops systems and procedures to detect, monitor and report the riskier customers and transactions, it will increase its chances of staying out of harm's way from criminals and from government sanctions and penalties.

A risk-based approach requires institutions to have systems and controls that are commensurate with the specific risks of money laundering and terrorist financing facing them. Assessing this risk is, therefore, one of the most important steps in creating a good anti-money laundering compliance program. As money laundering risks increase, stronger controls are necessary. However, all categories of risk — whether low, medium or high — must be identified and mitigated by the application of controls, such as verification of customer identity, CDD policies, suspicious activity monitoring and economic sanctions screening.

[7] http://bankingjournal.aba.com/2016/01/aba-challenges-cost-benefit-analysis-of-customer-due-diligence-proposal/

Governments around the world believe that the risk-based approach is preferable to a more prescriptive approach in the area of anti-money laundering and counter-terrorist financing because it is more:

- **Flexible** — as money laundering and terrorist financing risks vary across jurisdictions, customers, products and delivery channels, and over time.

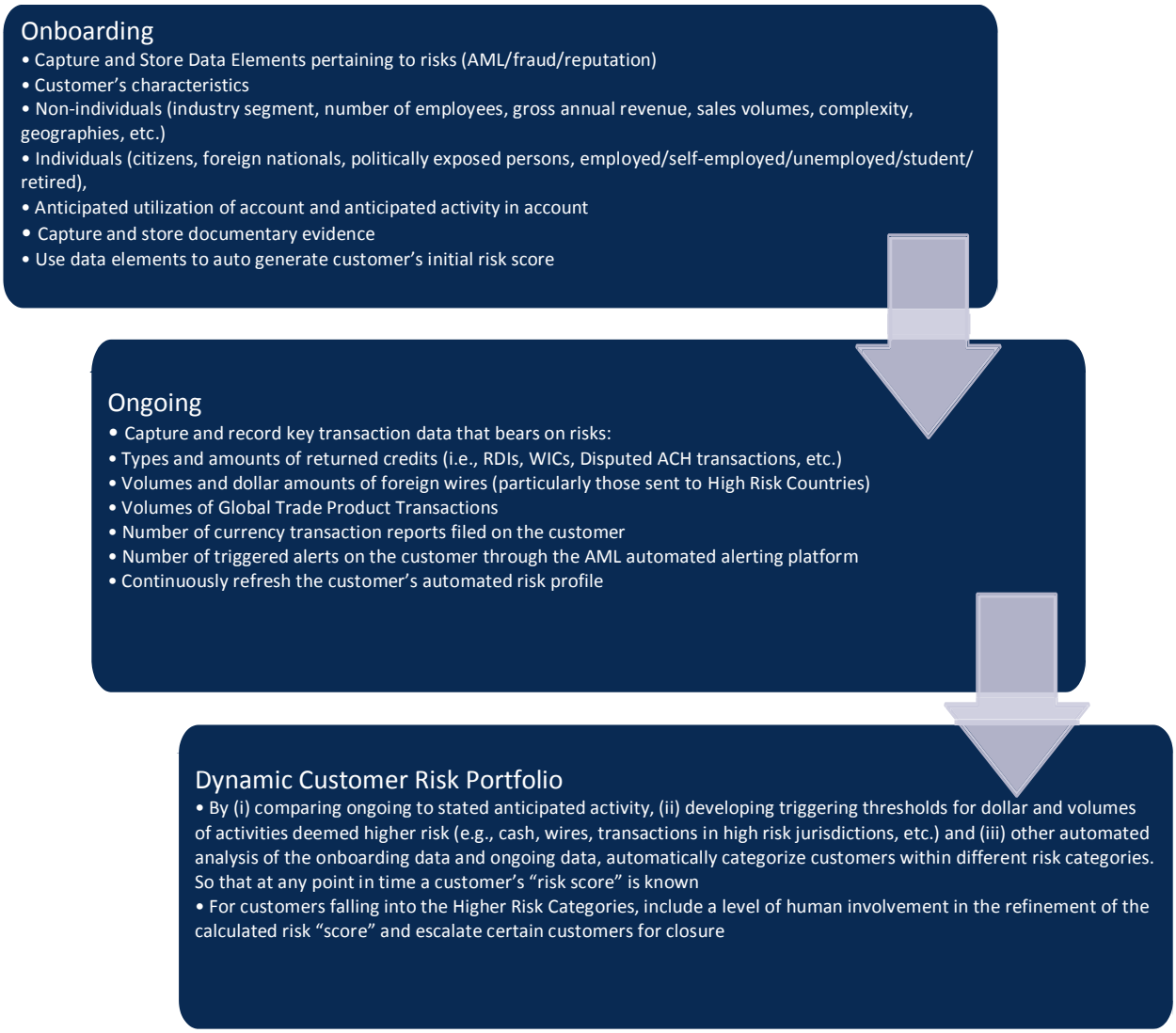
- **Effective** — as companies are better equipped than legislators to effectively assess and mitigate the particular money laundering and terrorist financing risks they face.

- **Proportionate** — because a risk-based approach promotes a common sense and intelligent approach to fighting money laundering and terrorist financing as opposed to a "check the box" approach. It also allows 186 Study Guide for the CAMS Certification Examination firms to minimize the adverse impact of anti-money laundering procedures on their low-risk customers.[8]

Depending on the risk score of a customer monitoring/EDD should be a risk-based approach and is taken as it pertains to CDD/EDD, approval and monitoring of high-risk customers. A financial institution's customers risk scoring model (Model) may be further stratified into tiers (e.g., Low, Moderate and High) to more effectively assess the different degrees of risk that customers may pose to a financial institution.

Vision of a Dynamic, Customer Risk Scoring Process:

[8] http://files.acams.org/pdfs/English_Study_Guide/Chapter_4.pdf



The Model serves as a fundamental component in the identification of high-risk customers. It should be developed to ensure that a firm has a robust CDD/EDD program in place that aligns with the institution's risk profile, allowing for consistent customer risk scoring across the institution that aids in the development of a central oversight function pertaining to due diligence practices.

A securities firm or financial institution's general policy for conducting CDD/EDD should also include assessing and scoring the risks associated with customers and entities. In addition, customers that fall within specific higher risk scores should be subject to further scrutiny.

The History:

When securities firms and financial institutions were found to have inadequate BSA/AML programs, specifically lacking in risk assessment or a formal CDD program, they were subjected to large fines and the reputation of those financial institution suffered greatly through public exposure. In 2014 fewer firms

received fines for AML violations, however, the total dollar amount of the fines increased significantly compared to 2013. The monetary amount of settlements for money laundering, tax evasion and sanctions levied by regulators and law enforcement agencies exceeded $13 billion in 2014.

The Benefits:

However costly and time consuming AML compliance may be, financial institutions that understand the importance of implementing a strong AML program will quickly realize its worth. In today's world, any financial institutions who do not appreciate the importance of a strong BSA/AML programs targeting customer risk scoring and CDD programs need to understand the costs and risks of having an inadequate AML program. When you have a strong AML program, the risk of financial loss due to penalties can be mitigated along with various other regulatory, legal and reputational risks.

The Problem:

In cases where a securities firm or financial institution is lacking a systematic CDD program, it may hinder a firm from risk scoring customers and entities, or from performing EDD that will allow the institution to identify high-risk relationships at the point of onboarding and performing ongoing due diligence in an efficient manner. When a securities firm or financial institution lacks the appropriate customer risk scoring controls or a formal CDD program, the reputational risk of the firm can be elevated. Securities firms and financial institutions that do not have a formal CDD program and customer risk scoring model may be unnecessarily exposing themselves to large BSA/AML sanctions and fines should its customers conduct illegal transactions through the institution.

How it works:

A securities firm or financial institution's BSA/AML compliance program should have comprehensive customer risk scoring and CDD policies, procedures and processes that are reasonably designed to:

- Provide a customer risk score,
- Verify the customer's identity, and
- Assess the risk associated with that customer as it pertains to money laundering and terrorist financing.

When customer risk scoring or CDD has identified heightened risk, securities firms and financial institutions' policies, procedures and processes should subject the customer to closer scrutiny that would require at a minimum EDD and ongoing monitoring. Customers who are identified as presenting a higher level of risk to an institution should be monitored by your high risk customer team or department.

Risk scoring a customer or entity when onboarding an account allows securities firms and financial institutions to properly evaluate the risk associated with each new account, and allow the firm to adjust a risk score though ongoing monitoring of account activity and account information updates. This can be accomplished by documenting a baseline that will be used to determine what type of activity is not in line with the customer baseline that may need to be reported when monitoring customer transactions for suspicious activity.

Not all customers or entity accounts will be assigned a high risk score though the risk scoring process during onboarding. However some accounts may be flagged as a higher risk scored account through ongoing monitoring based on a baseline formed from the CDD collected during onboarding:

Examples of "individual" KYC questions that may determine a higher risk score when onboarding are:

- Are you a citizen of any other counties?
- If yes, of which country are you a citizen?
- Do you have a current Visa status?
- Do you have address (physical, P.O. Box, etc.) in a foreign country?
- Do you currently hold or have you previously held a position as a senior political official in any form of government?
- If yes, for what country is the associate's position held?
- Do you have a family member or close associate who currently serves or have they formerly served a high position as a senior political official in any form of government?
- Have you been a U.S. Citizen for less than 5 years?

You may also assign new or existing accounts a higher risk score based on the following CDD information:

- Source of funds
- Purpose of the account
- Anticipated ACH/FFW deposit activity
- Anticipated ACH/FFW withdrawal activity
- High-risk jurisdictions transactions
- Anticipated account transaction activity
- Anticipated vs. actual volume and types of transactions
- Customer's ownership structure on entity accounts
- Business ownership of the customer's
- Source of customer wealth
- For entity accounts the beneficial owners of the accounts, and
- For entity accounts the customer's (or beneficial owner's) occupation or type of business

Accounts assigned a higher risk score should be subject to enhanced due diligence by requesting the following information or documents, as applicable, in order to effectively evaluate the risk presented by that customer and to detect and report suspicious activity.

- Financial statements
- Banking references
- Domicile (where the business of your customer is organized)
- Explanation of customer's primary trade area's and if your costumer is anticipating routine international transactions
- Explanation of the business operations and expected volume of trading, and;
- Explanations for any variations in account activity.

It is an important part of a securities firm and financial institution's AML and suspicious activity report (SAR) reporting program to obtain necessary information about each customer to allow your firm to evaluate the potential risk presented by that customer in order to identify and report suspicious activity in a timely manner. When a securities firm or financial institution is onboarding a new account for a customer, the risk scoring and due diligence that is performed should be part of the customer information obtained for your CIP purposes.

The standards of an effective BSA/AML compliance program applying customer risk scoring and customer due diligence policies, procedures, and processes are founded upon the following four elements:

The reputation of financial institutions will be better protected and will benefit from this type of risk-based approach providing the institution has developed detailed policies, procedures, and processes outlined around the model and implementation of your risk scoring parameters.

Examples:

Securities firms and financial institutions may consider customers high risk when they score High according to the customer risk scoring and CDD policies, procedures and processes, and the scoring parameters outlined in firm policies. Policies should be reviewed regularly and may need to be amended from time to time by your BSA officer or designated individual. A customer that falls within a specific risk category as defined by a institutions customer risk scoring and CDD policies, procedures and processes will be determined by their risk score, and may consider using regulatory guidance such as that outlined in the FFIEC Examination Manual. Below are some examples from the FFIEC Examination Manual:

High (CDD Model- Risk Score): A customer scoring High via the Model is defined as one that is more vulnerable to money laundering or terrorist financing due to the type of customer and/or type of service/product used by the customer.

Moderate (CDD Model-Risk Score): A customer scoring Moderate via the Model is defined as one that could be vulnerable to money laundering or terrorist financing. However, due to the nature of the services offered by the bank or the products and services used by the customer, the money laundering and terrorist financing risk is moderate.

Low (CDD Model- Risk Score): A customer scoring Low via the Model is defined as one that poses lower level of risk associated with money laundering or terrorist financing. This customer does not significantly impact the overall risk of the bank.

Financial institutions may benefit by developing a baseline to quantify customer risk scoring parameters programs and further categorize higher risk customers into high risk tiers to identify the need for ongoing monitoring of higher risk scored customer transactions for suspicious activity.

Example of Customer Risk Scoring Parameters:

- Risk Score of Low = 0 to 79 points
- Risk Score of Moderate = 80 to 99 points
- Risk Score of High = 100 points or greater

Example of High Risk Tier Parameters:

- High-Low = 100 to 150 points
- High – Moderate = to 151 to 199 points
- High – High = 200 points or greater

The Solution:

Financial institutions must insure that they have implemented a strong BSA/AML compliance program and subject-matter training that adequately supports a formal CDD process and customer risk scoring, specifically through an independent risk assessment. Your financial institution will greatly benefit from developing and implementing a formal CDD process and customer risk scoring (Model) to effectively mitigate exposure of reputational risk by preventing possible unusual or suspicious transactions that may expose your financial institution to monetary losses or increased expenses. While this solution may not be suitable for all financial institutions, your institutions management needs to have a thorough understanding of the risks of its customer base and develop the implementation of documented policies and procedures to adequately mitigate money laundering.

What to look for when considering solutions:

Almost all securities firms and financial institutions will benefit from the information found in the FFIEC BSA/AML Examination Manual by reviewing the BSA/AML Risk Assessment – Overview.

"Objective. Assess the BSA/AML risk profile of the bank and evaluate the adequacy of the bank's BSA/AML risk assessment process.

The development of the BSA/AML risk assessment generally involves two steps: first, identify the specific risk categories (i.e., products, services, customers, entities, transactions, and geographic locations) unique to the bank; and second, conduct a more detailed analysis of the data identified to better assess the risk within these categories. In reviewing the risk assessment during the scoping and planning process, the examiner should determine whether management has considered all products, services, customers, entities, transactions, and geographic locations, and whether management's detailed analysis within these specific risk categories was adequate. If the bank has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the bank has not

completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment based on available information."[9]

The following areas of information are key areas to focus on when calculating the suitability of your financial institution's BSA/AML risk assessment process. This is essential when considering your securities firm or financial institutions BSA/AML compliance program and risk profile:

- Evaluating your financial institutions BSA/AML risk
- Identifying specific product risk categories
- Evaluating specific products and services risk
- Evaluating customers and entities specific risk rating
- Identifying geographic location risk
- Evaluating your CDD/EDD process
- Evaluating customer risk scoring process
- Review independent risk assessment

Specific solutions:

All securities firms and financial institutions must have a clear understanding of their BSA/AML risk exposure by developing CDD and customer risk scoring policies, procedures and processes to monitor and control BSA/AML risks. For example, your institution can implement monitoring systems to identify, research and report suspicious activity. The most effective program will be based on CDD and customer risk scoring, with particular emphasis on higher risk products, services, customers, entities and geographic locations as identified by your institutions BSA/AML risk assessment. All securities firms and financial institutions should request independent testing (audit) to review your BSA/AML program risk assessment for reasonableness and compliance. Securities firms and financial institutions may realize a need to increase staffing along with additional subject-matter training in order to promote adherence with its own BSA/AML policies, procedures and processes.

For specific guidelines and solutions regarding CDD, customer risk scoring, and higher risk customers, securities firms and financial institutions are advised to consult the FFIEC BSA/AML Examination Manual and review the CDD – Overview.

"Objective: Assess the appropriateness and comprehensiveness of the bank's customer due diligence (CDD) policies, procedures, and processes for obtaining customer information and assess the value of this information in detecting, monitoring, and reporting suspicious activity.

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 higher risk for money laundering and terrorist financing. The objective of CDD should be to enable the bank to predict with relative certainty the types of transactions in which a customer is likely to engage. These processes 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.

[9] https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_005.htm

Processes should also include enhanced CDD for higher-risk customers and ongoing due diligence of the customer base.

Customer Due Diligence Guidance

BSA/AML policies, procedures, and processes should include CDD guidelines that:

- Are commensurate with the bank's BSA/AML risk profile, paying particular attention to higher-risk customers.
- Contain a clear statement of management's overall expectations and establish specific staff responsibilities, including who is responsible for reviewing or approving changes to a customer's risk rating or profile, as applicable.
- Ensure that the bank possesses sufficient customer information to implement an effective suspicious activity monitoring system.
- Provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.
- Ensure the bank maintains current customer information.

Customer Risk

Management should have a thorough understanding of the money laundering or terrorist financing risks of the bank's customer base. Under this approach, the bank should obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. This understanding may be based on account type or customer classification.

Enhanced Due Diligence for Higher-Risk Customers

Customers that pose higher money laundering or terrorist financing risks present increased exposure to banks; due diligence policies, procedures, and processes should be enhanced as a result. Enhanced due diligence (EDD) for higher-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank's reputation, compliance, and transaction risks. Higher-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank."[10]

It is crucial that all securities firms and financial institutions understand that CDD and risk scoring a customer or entity is an ongoing process, and firms must take measures to ensure account profiles are current and monitoring is risk-based. Securities firms and financial institutions should consider how or when risk profiles should be adjusted and ensure suspicious activity is identified when the activity is not consistent with a customer profile.

[10] https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_005.htm

Conclusion:

Securities firms and financial institutions that have completed independent risk assessment and assume a higher-risk BSA/AML profile, should definitely consider implementing a more robust BSA/AML compliance program that specifically monitors and controls the higher risks that have been identified, in addition to adding enhanced CDD and customer risk scoring policies, procedures and processes.

The initial identification of a high-risk customer may occur at any time during the life cycle of a customer's relationship with a financial institution, but should ideally occur upfront during the account opening process. At account opening, customers are asked KYC/CDD questions that will allow your financial institution to establish knowledge of the customer and their anticipated account activity. If a customer falls within a certain category, additional dynamic questioning will be triggered.

Depending on whether the account is for an individual, a business, or other entity, targeted KYC and CDD information should be obtained, including but not limited to employment status, residency, source of wealth, anticipated account activity and purpose of account. If the customer falls within one of the higher risk categories (as defined by your BSA/AML compliance program), your institution will collect additional documentation from the customer as outlined in your due diligence processes. As such, securities firms and financial institutions should have formal policies and procedures in place (approved by the BSA/AML officer) to identify customers that fall within higher risk categories and collect required documentation during the onboarding process and when high-risk customers are identified during ongoing monitoring.

Any suspicious activity detected by your financial institution along the course of the initial CDD/EDD efforts or the ongoing monitoring process that may require further review should be escalated to evaluate the potential risk presented by that customer in order to identify and report suspicious activity. Based on the outcome of the investigation, your firm should make a definitive decision regarding the closure of the customer relationship including filing a SAR with FinCEN, if warranted.

Federal and/or state regulatory agencies will periodically examine institutions to ensure they are in compliance with the law. Regulatory agencies may also coordinate with each other to minimize the variation in how they each interpret the laws and rules. A financial institution will greatly benefit by having formal written policies and procedures that document how the firm securely stores this information (i) as evidence of compliance with customer identification requirements; (ii) to evaluate risks that customers may pose to the firm; and (iii) to protect the financial institution and its customers when conducting investigations into potentially suspicious transactions.