WHITE PAPER

IMPROVING INVESTIGATIONS THROUGH THE CDD AND EDD PROCESS

Written by: | Tyler Nicoll 2015
# Table of Contents

**EXECUTIVE SUMMARY** .................................................................................................................. 2

**CUSTOMER IDENTIFICATION PROGRAM** ...................................................................................... 3

**CUSTOMER DUE DILIGENCE** ........................................................................................................... 4
  - Risk Rating Customers ..................................................................................................................... 4
  - Beneficial Ownership ....................................................................................................................... 5
  - Lack of Information .......................................................................................................................... 6

**ENHANCE DUE DILIGENCE** ............................................................................................................ 6
  - Customize EDD ............................................................................................................................... 7
  - Review the Relationship .................................................................................................................. 7
  - Available Information ...................................................................................................................... 8
  - Update Account Profile .................................................................................................................... 8
  - On-Site Visitations ........................................................................................................................... 8
  - Form 8300 ......................................................................................................................................... 9
  - Independent Audits for MSBs and Special Dealers ......................................................................... 9
  - Negative New Searches .................................................................................................................... 10
  - Leveraging Loan Information .......................................................................................................... 10
  - Document and Support Analysis .................................................................................................... 10

**INCORPORATING THE CDD/EDD INTO SAR INVESTIGATIONS** ...................................................... 10
  - System Limitations ......................................................................................................................... 11
  - SAR Reviews .................................................................................................................................. 11

**CONCLUSION** .................................................................................................................................. 11
Executive Summary

Regulatory expectations to satisfy Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) regulations continue to evolve in the U.S. and an essential component of an adequate BSA/AML program includes the responsibility for institutions to adequately know its customer base. Most institutions have effectively incorporated their regulatory responsibilities into their business plans to ensure that they have an adequate program, including a qualified BSA officer and resources, sufficient control mechanisms, appropriate training and robust independent testing. Those institutions that have implemented a strong system to identify, measure, manage, monitor and control their BSA/AML risks have met ongoing compliance requirements and current regulator expectations (as discussed in the forms of Financial Institution Letters, the BSA/AML Examination Manual, etc.). However, those institutions that place less than satisfactory emphasis on compliance have encountered the implications and potential penalties associated with those decisions. In 2014, the FDIC alone placed 15 institutions under Consent Orders for weak customer due diligence (CDD) and enhanced due diligence (EDD) standards and/or inadequate suspicious activity monitoring and reporting.

Regulations and guidance help establish the first line of defense for an institution through a Customer Identification Program (CIP) and CDD processes. The CIP regulation establishes minimum required standards for each banking customer, but should never be considered adequate information for knowing and understanding a customer’s account activities. CIP establishes minimum, risk-based methods for gathering key, discernable information to properly identify their customers. The CDD process builds upon the CIP data, and should be designed to gather additional customer information to assist in properly risk rating customers and identifying those banking relationships that pose higher money laundering or terrorist financing risk. CIP and CDD standards are an important first line of defense for any institution; however, there may be high-risk customers, activities, transaction behaviors, geographies that pose additional risk and warrant additional due diligence, often termed as EDD.

As described in the BSA Manual, “Customers that pose higher money laundering or terrorist financing risk present increased exposure to the banks,” and should receive more due diligence. EDD should provide the institution a more in-depth understanding of the customer’s activities than what is typically gathered through the standard CDD process.

Most institutions also incorporate some type of software programs to assist them in monitoring accounts for unusual or suspicious activities and to verify information relating to the Office of Foreign Assets Controls (OFAC) restrictions, 314(a), or other watch lists. Depending upon the sophistication and capabilities of the software for suspicious activity monitoring, management may have daily, weekly, or monthly reports that aggregate customer information or an automated system that will monitor account activities and generate “alerts” for suspicious activity.

Underlying CDD and EDD information is essential in the bank’s review of the activities or alerts to support an understanding (or lack of) the transactional activity. CIP, CDD, and EDD data

---

1 FFIEC BSA/AML Examination Manual Page 57
elements can also be crucial in matching customers to OFAC, 314(a) and other watch lists since simple name matches are very common.

Communication and sharing of customer information within the bank is essential. Investigators reviewing transaction activities or alerts may lack an understanding of the activity in an account when explanations are clearly explained within the customer loan files or other sources within the institution. Sharing of such information minimizes the filing of unnecessary suspicious activity reports (SARs) and should minimize redundancies and information and data collection duplication within different departments or divisions of the institution.

The purpose of this paper is to encourage institutions to enhance the information sharing processes among departments to create a more efficient suspicious activity monitoring process. In particular, this paper will demonstrate how to improve efficiencies within the suspicious activity review process by utilizing in-house information mostly gathered during the CDD and EDD processes.

### Customer Identification Program

The first step in understanding customers is to identify them. The CIP rule requires four pieces of information that an institution must gather to demonstrate knowledge of its customers.

- Name
- Date of birth
- Residential or business address (an Army or Fleet Post Office box number or residential address of next of kin or other contact may be substituted)
- Identification number

Identifying domestic residents is simpler when documentation is issued by a local or federal agency. Although gathering such information is basic, it is the responsibility of the institution to build a “reasonable belief that it knows the true identity of each customer.”2 One of the hardest things for institutions is to properly identify customers, due to the risk of identity theft. In 2012, 1.1 million individuals had their information misused to open up new bank accounts, and about 833,600 persons had their information misused for other fraudulent purposes.3 The bank need not establish the accuracy of all information obtained;4 however, to protect the institution from obtaining false information, management can train their employees using the U.S. Department of Justice’s “Law Enforcement Guide to False Identification and Illegal ID Use”5 or utilize a third-party system to verify data using knowledge-based questions—the answers to which only the customer should know.

---

2 FFIEC BSA/AML Examination Manual Page 47
3 [http://www.bjs.gov/content/pub/press/vit12pr.cfm](http://www.bjs.gov/content/pub/press/vit12pr.cfm)
4 FFIEC BSA/AML Examination Manual Page 49
Utilizing a data verification system is one of the best ways in combating false identification. In the past, only online banks would use data verification to verify new customer account information; however, more traditional institutions are taking precautionary measures by verifying customer information using third-party systems, better protecting them from false or stolen identification.

For foreign/nonresidential aliens, the requirements do not change. International individuals typically do not have state or federal identification, but have valid passports or other official government identity documents which bear a photo or fingerprint to verify identity. Management can utilize individual passports or other suitable forms of official government documentation to verify identity. If an institution deals heavily with foreign/nonresidential aliens, World-Check’s passport check can assist in identifying fake passports.

Businesses are harder to verify through a third-party provider. Most states do not require full ownership disclosure, which makes it appealing for individuals to establish shell companies that can assist them in laundering money, evading taxes, or conducting other illicit activities with little chance of the underlying beneficial owner being identified. Requiring additional information at account opening is one way to ensure that businesses are established for legal purposes, as further discussed below.

Customer Due Diligence

Risk Rating Customers

Establishing an effective CDD program is another cornerstone to implementing an effective BSA/AML program. Once an institution has established the customer’s identity, it is critical for an institution to continue understanding their customers through proper due diligence. The BSA/AML examination manual refers to a risk-based approach in establishing and monitoring accounts. The institution should establish basic questions that should be asked at account opening. Some of these questions should be used to understand the following information, but is not limited to:

- Occupation or type of business
- Purpose of the account
- Products and services that will be utilized
- Anticipated activity volumes
- International transaction frequency
- Nationality or place of formation/incorporation

Currently, there is no requirement for an institution to monitor account activity and customer risk profiles through an automated system. Regardless, bank management is responsible for ensuring proper oversight, not only at account opening, but throughout the customer relationship. By establishing basic questions, the institution will understand the anticipated activity and other traits (risk factors) that will enable the institution to identify potentially higher risk customers. These traits can include higher-than-normal anticipated wire transactions to a foreign country or large
amounts of cash deposited or withdrawn within a short time period. Whatever the customer initially stated, a risk rating should be assessed using the factors as discussed above, and periodically reviewed for proper understanding of the individual or business activities. For accounts that are manually risk rated, it is best for any institution to review new account activity, typically six months after account opening, to ensure that account activity has not deviated from the initial CDD. If material deviations have occurred, a reasonable understanding should be gathered and documented. The BSA officer can re-evaluate the risk rating and adjust the rating according to the activity or services now rendered. This can also assist the BSA officer in determining to close the account due to behaviors outside of the bank’s risk tolerance.

For those institutions that have implemented a more sophisticated system, it becomes easier to monitor. After significant development and testing of system parameters, the new account representative will input the CDD, and the BSA officer will have the system work for them. The system should aggregate account activity and compare it against parameters and rule sets, against the anticipated activity input at account opening, or a combination (depending on the capabilities of the system) of the two. If the activity has materially deviated or is otherwise unusual, an alert should be generated (based on management’s pre-determined level of deviation or set parameters) and reviewed.

Automated systems may also incorporate or offer a customer risk-rating module, which risk-rates the customer based on the activity during that time period (typically quarterly but sometimes monthly). Through this process, the institution can establish designated thresholds that will help them identify low, moderate and high-risk customers and perform more due diligence when needed.

**Beneficial Ownership**

In 2010, FinCEN sent out guidance stating that “based on the financial institution’s risk assessment of a new account opened by a customer that is not an individual, a financial institution may need to take additional steps to verify the identity of the customer seeking information about individuals with ownership or control over the account, including signatories.” However, institutions are still waiting on a final ruling, which is expected to require additional identification and verification of share owners of a company to owners of the actual assets. While institutions wait on the final ruling, the institutions are still required to develop an understanding of the identity of beneficial owners of a corporation, account owned by a legal entity, or trust accounts. The first step in properly implementing such requirements is to ensure their systems are capable of recording multiple beneficiaries or ownerships. Second, management should establish their own guidelines based on their understanding of the 2010 guidance. In the meantime, bank management can look to international guidance set by the EU Directive 2015/849 or the New Zealand Federal Reserve of ownership of 25 percent or more for verifying such owners.

---

Management should also be aware of the certain entities identified as higher risk in the 2010 FinCEN guidance (corporate and shell entities, private or personal investment companies, and trust companies) and the specific guidance given for certain situations. The guidelines state:

“…as part of an institution’s BSA/AML compliance program, a financial institution should establish and maintain CDD procedures that are reasonably designed to verify the identity of beneficial owners of an account, as appropriate, based on the institution’s evaluation of risk pertaining to an account.

For example, CDD procedures may include the following:

- Determining whether the customer is acting as an agent for or on behalf of another, and if so, obtaining information regarding the capacity in which and on whose behalf the customer is acting.

- Where the customer is a legal entity that is not publicly traded in the United States, such as an unincorporated association, a private investment company (PIC), trust or foundation, obtaining information about the structure or ownership of the entity so as to allow the institution to determine whether the account poses heightened risk.

- Where the customer is a trustee, obtaining information about the trust structure to allow the institution to establish a reasonable understanding of the trust structure and to determine the provider of funds and any persons or entities that have control over the funds or have the power to remove the trustees. 9

Lack of Information

Institutions can open up accounts without having all previously mentioned documentation in hand. However, management should be cautious in giving full customer access to accounts until all documentation is received. Management should establish policies and procedures about handling such circumstances, terms under which a customer may use an account while the bank attempts to verify the customer’s identity, and when the institutions should close an account, after attempts to verify a customer’s identity have failed. 10 The more access granted to such customers, the more vulnerable the institution becomes to potential money laundering.

Enhance Due Diligence

Customers that pose higher money laundering or terrorist financing risk present increased exposure to the institution. As previously discussed, management should monitor its customer base and properly risk rate those customers. Those customers rated higher risk should receive further due

9 http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-g001.pdf - Page 2 and 3
10 FFIEC BSA/AML Examination Manual Page 50
diligence to ensure that the company or individual is acting within its legal limits and that the sources of those funds are from legitimate sources. Institutions should factor in customers that are named subjects in recent SAR filings. These individuals are typically placed on the high-risk list for a period of time and once EDD is performed on them, may be removed if activity reverts back to normal.

The 2014 FFIEC BSA/AML Examination Manual states “as due diligence is ongoing, a bank should take measures to ensure account profiles are current and monitoring should be risk-based.”

Knowing this, the institution should periodically review its high customer list and update the customer profiles. The more the institution has become familiar with its high-risk customers, the less frequent these reviews should occur; however, this review should never stop just because the institution becomes familiar and comfortable with a customer’s transactions. From a risk perspective, if the customer continues with high-risk transactions, it does not warrant a downgrade in a risk rating simply because the institution has accepted the higher risk transactions as “normal activity.” However, from a risk-based perspective, an institution could extend the review cycle out so as to ensure that, on a less frequent basis, the customer is still operating within expected parameters.

**Customize EDD**

EDD guidelines and expectations have evolved over time and current regulations have not kept pace with those guidelines. One way to keep current about regulatory guidance and industry best practices is to speak with other institutions. Management can also review recent Consent Orders pertaining to BSA in order to gain an understanding of current failures. While performing EDD, management should be cognizant that some of the requested information could be in-house and readily available for review. Customers that have any borrowings with the institution provide a wealth of financial information for the underwriter. The BSA/AML compliance team could benefit from such information when performing due diligence (or suspicious activity investigations) and determining the reasonableness of account activity.

Before discussing periodic reviews of higher risk customers, the reader should note that there is not a “one-size fits all” review. Each business or individual is unique. While businesses and customers can be compared, one cannot argue that a hot dog stand business is similar to an international trade business. Even among hot dog sellers, there can be a large difference in account behavior depending on the specifics of that business (do they have a cart or an upscale hot dog eatery). Knowing that, not all analyses should be the same. Although there may be similar traits and attributes (reviewing trends and variances within the account), the institution should customize reviews based on the customer’s risk profile and account activities.

**Review the Relationship**

Understanding the entire relationship is crucial. The analyst should be aware of all affiliates and related parties at the institution and use judgment to determine the extent of the review. For example, if the owner has 10 different businesses and two are on the high-risk list, it is best practice
to understand if those businesses truly operate independently or if there is frequent intermingling of funds indicating that the risk (and periodic reviews) should be at the relationship level. In addition, if suspicious activity is identified in one business, it is more likely that other related businesses may exhibit similar behavior.

Furthermore, while reviewing such entities, management should look at the underlining beneficiaries of the companies.

**Available Information**

Do not waste time re-inventing the wheel. When an individual walks in the door, a large amount of information is gathered on the individual or business. If an individual or business customer applied for a loan or other services, then that department probably requested more information on their financial condition. This could be beneficial in reviewing the account information and verifying the sources of their income or wealth.

**Update Account Profile**

Ideally, a new account packet contains information explaining the type of account activity that a customer will be doing over the year. This creates a baseline for management to compare against. When large deviations occur, management should seek to clarify these differences and update the account information for the next review. For moderate or low-risk customers, such information becomes outdated or obsolete. Management should ensure account information is updated when needed (for example, unexplainable activity from a suspicious activity investigation may be an ideal time to update information).

**Onsite Visitations**

Performing onsite visitations could be one of the best practices to truly understanding high-risk customers. For institutions that have implemented such processes, management should be conscious that regulators have recommended the establishment of “guidelines for on-site visitation of high risk customers” in recent Consent Orders. By implementing these guidelines, the institution’s representative can uncover activities, or products and services, that the customer failed to disclose at account opening. Bank management could benefit from normal routine visitations from the credit department. If properly trained, the sale or loan reviewer can not only identify normal business activities, but can also uncover potentially suspicious activity and document that review for the BSA department. The review focus should consider documenting appearance of signage in and around the facility, any recently acquired facilities, onsite ATMs, shared office space with other businesses, and establish a general sense of customer presence. If it is a cash-intensive business the employee should question if the customer’s traffic flow reflects the amount of cash deposited or if the building remains empty when the customer’s deposit behavior reflects differently. Another area that is becoming more relevant is the company’s inventory. As the representative walks through for the onsite visit, he should question if the inventory is properly rotated or if they have outdated products that appear year after year in their annual or semi-annual

---

12 Consent Order for Seaway Bank and Trust Company, Chicago, Illinois – FDIC-14-0147b
onsite inspection. Placing such scrutiny on inventory may also assist in mitigating credit risk to the institution. Although noted inconsistencies do not necessarily equate to suspicious activity, it should raise a level of concern and further inspection.

While onsite or while the customer is at the institution, bank representatives should hold periodic discussions with business owners to see if they are expanding their business or venturing into any new business lines. No matter how minor the changes, it could help the EDD process immensely.

Form 8300

Some institutions house cash-intensive customers where proceeds come from sales of high-priced items including automobiles and airplanes. Companies that accept customer payments in excess of $10,000 must file a Form 8300 with the U.S. Treasury Department. Even though they are required by law to make this filing, there have been multiple instances where companies have neglected to file these forms and ended up paying large settlements for such actions. John Frank Mussari (48) was the former owner of Mussari Motors Inc., in San Diego, California and plead guilty to conspiracy to evade filing Form 8300's. Mussari admitted to receiving cash payments of $132,000 for a Ferrari 360 Spyder, $147,000 for a Porsche 911 Turbo Cabriolet, and $320,000 for two Lamborghini Gallardos. Mussari probably knew that the cash-rich buyers were receiving the funds from illicit sources but “he never inquired about the source of the cash,” according to the plea agreement. Institutions might not have caught such a scheme as Mussari held $205,000 of the cash at his establishment; however, he most probably deposited the remainder of the funds. Cash deposited into an account might appear as legitimate; however, bank management can take a risk-based approach to inquiring or even gathering documentation on customers depositing high levels of cash especially when they purportedly sell goods that easily cost more than $10,000.

Independent Audits for MSBs and Special Dealers

As previously mentioned, it is best practice to ensure each EDD is customized to the specific business entity. The Treasury issued multiple regulations that require certain entities (MSBs and dealers in precious metals, stones, or jewelry) to have an AML program, yet most banking institutions do not inquire of such programs or receive certification from such companies that a program even exists. While it is a good idea to gather such information at the account opening, management should check that these customers have a risk-based AML program during the high-risk EDD review process. Part of the interim final rule (frequently asked questions), Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels, question 4(a)4 states that those companies that fall underneath the definition of “dealer” should have someone independently reviewing the AML program and ensuring the adequacy of the program. Similar requirement to obtain independent reviews are for money services businesses (MSBs). If the institution has a high-risk customer that falls within the definition of “dealer” of precious metals, management could request a copy of the most recent independent review of its AML program.


This not only ensures the customer is following federal laws, but it could also mitigate some regulatory risk.

**Negative New Searches**

A negative news search is an easily performed task that provides somewhat indisputable information. Should any adverse information be discovered, the reviewer should document the results and escalate the issue to the BSA officer for secondary review. Also, keep in mind that it is important to understand a high-risk customer’s primary clients and suppliers, if any. The reviewer, using a risk-based approach, may want to ensure the high-risk customer’s vendors’ or customers’ business activities align with the high-risk customer’s business purpose. They may also want to perform Internet searches on a select number of the high-risk customer’s funds transfer recipients. The reviewer could discover that the institution’s customer is sending large transactions to an entity that the customer would not normally be expected to engage in, and management knows of no reasonable explanation for the transaction after examining the available facts, including the background and purpose of the transaction. The reviewer could find a uniform manufacturer sending large amounts of wires to a fish wholesaler.

**Leveraging Loan Information**

Another helpful tool is to review account activity and ensure that it falls closely in line with the individual’s tax return. Most individuals or businesses do not give up their tax returns simply for institutions to review for suspicious patterns; however, most loans have covenants that require updated, annual tax returns. If a high-risk customer also has a loan at the institution, it would be wise to pull the most recent tax return and compare it with account activity.

**Document and Support Analysis**

The most important thing an institution can do to avoid regulatory criticism is document and support all information placed in the EDD. This will not only avoid criticism, it will also help the subsequent EDD reviewer and give them guidance on the previous conclusion.

**Incorporating the CDD/EDD into SAR Investigations**

The larger or more complex the institution, the more sophisticated the BSA department should become. Larger institutions develop specialty areas within the BSA department. For example, investigative teams are created to review the alerts from the suspicious activity software, escalate some to cases for investigations and possible SAR filings. Other teams may be established to file SAR’s on ongoing suspicious activity, file CTRs and perform periodic reviews on high-risk customers. However, information sharing may become harder and inefficiencies may start to surface with such divisions of responsibilities. Smaller institutions typically do not have such issues as there are typically one or two individuals overseeing the entire BSA function.
**System Limitations**

Depending on system interfaces, some institutions will run into issues with accessing information. Not only will the BSA department need access to loan review presentations and financial information but they will also need to understand how to navigate around the software to access additional information, which typically require additional training. For larger institutions, this could get more complex as institutions might be running more than one system for loan imaging and storing.

**SAR Reviews**

When investigators review alerts for unusual behavior, it is important that they use all available information at the institution. One of the best sources of information for any investigator is reviewing the most recent due diligence. This information would hopefully inform the investigator of trends and average monthly balances for the customer. Although the investigator may start with the account that alerted, he should always follow the money to ensure that activity is commensurate with the overall business model. Investigators might find some activity to be suspicious at first but, when reviewing the EDD, will determine that the activity is normal such as a seasonal business causing a sudden increase in activity. Investigators should ensure that they follow the money from all accounts.

**Conclusion**

Improving information sharing can only improve the overall efficiency of the SAR review process. Also, performing thorough EDD on high-risk customers and utilizing that information when performing other important analyses should improve the efficiency of an investigation and assist in making quicker decisions and determinations. This will also improve SAR reporting as more quality SARs will be delivered to local and federal authorities, while eliminating unnecessary SARs.