White Paper

Anti-Money Laundering policy guidelines

August 2014

Risk Solutions

Table of Contents

Anti-Money Laundering policy guidelines

Without the proper anti-money laundering (AML) compliance procedures, banks and other financial institutions are in danger of inadvertently facilitating drug trafficking, terrorism financing and other crimes. Financial institutions can be prosecuted for failing to have effective AML policies in place. This document provides an example of guidelines that can be used to create a due diligence program that detects potential money launderers within your customer base. In addition, the sample policy below is compliant with the USA PATRIOT Act and other similar legislation:

The institution's management will actively search for suspicious activity. When it is discovered, a representative officer will review it and make a recommendation as to whether a Suspicious Activity Report (SAR) should be filed.

A guideline for SAR reporting is that the assigned officer will usually have ten (10) business days to conduct the review and make his or her recommendation. Check the bank's SAR form for specific instructions. All recommendations will be made in writing and forwarded to the Bank Secrecy Act (BSA) Officer. The BSA Officer is responsible for reviewing the investigating officer's recommendation and determining if an SAR should be filed.

The BSA Officer will file the SAR with the appropriate legal and regulatory authorities. All supporting evidence for the SAR will be maintained for a minimum of five (5) years, and will be securely stored. The BSA Officer will report to the board of directors the number of SARs filed each month, along with a brief summary as to the dollar amount of the suspicious activities and why they were deemed as such.

Money laundering – Defined

1. It is the introduction of illegally obtained currency into the banking system.
2. It is using the banking system to illegally hide currency that was lawfully obtained. It is not hard for criminals to obtain currency. However, until the currency is deposited into the financial system, their ability to utilize it is restricted. When financial institutions knowingly accept the cash deposits of criminals, they legitimize (or launder) the proceeds. Accordingly, criminals must do business with banks. Those that offer Business Internet Banking services must be diligent in detecting and reporting suspicious activity.

Suspicious activity – Defined

It is impossible for management to define all activity that would qualify as suspicious. However, the following guidelines quantify the types of suspicious activities that the institution will monitor for.

Suspicious activity – Commercial accounts

1. One or more cash deposits a week that is structured to avoid currency transaction reporting (CTR). (Note: Structuring involves the repeated depositing or withdrawal of amounts of cash less than the $10,000 limit, or the splitting of a cash transaction that exceeds $10,000 into smaller cash transactions in an effort to avoid the reporting requirements.)
2. Two or more instances a week where a customer makes two or more cash deposits on the same day, and the total of the deposits is between $5,000 and $8,000.
3. One or more instances a week where a customer has made cash deposits to two or more related accounts, and the total of the deposits is between $5,000 and $10,000.
4. Cash deposits that are over $10,000, and that are 25% greater than the customer's second highest cash deposit.

5. Cash deposits that are over $10,000, and that are 150% of the customer's average cash deposits (ignoring inconsequential deposits that are below $3,000).
6. Cash withdrawals of more than $5,000, unless the withdrawal is made for payroll purposes.
7. Deposits or more than $3,000, made in traveler's checks or money orders.
8. Single purchase with cash of cashier's checks, traveler's checks or money orders for more than $5,000.
9. Purchase of a CD with cash for more than $5,000.
10. Deposits of more than $5,000 in a week, made primarily from wire transfers.
11. Check cashing customers, whose deposits of checks exceed by 50% the amount of cash they withdraw.
12. Two or more instances a week where small bills ($1, $5, $10, $20) or exchanged for large bills ($50, $100), in excess of $3,000.

Suspicious activity – Consumer accounts

1. Two or more deposits made during a week where the total amount of the deposits is greater than $5,000.
2. Two or more deposits made during a month where the total amount of the deposits is greater than $10,000.
3. Two or more cash deposits made during a quarter where the total amount of the deposits is more than $18,000.
4. Any cash deposit between $8,000 and $10,000.
5. Any cash deposit where the currency has a noticeable mildew aroma. Likewise, any cash deposit where the currency has an aroma that could be drug-related (e.g., alcohol, cannabis or an unidentifiable sweet smell).
6. One or more cash withdrawals during a month where the total amount is equal or above $5,000.
7. Deposits equal or above $3,000 in a day, made in traveler's checks or money orders.
8. Purchase with cash of cashier's checks, traveler's checks or money orders for $3,000 or more.
9. Purchase with cash of a CD for $3,000 or more.

Enhanced Due Diligence for new accounts

One of the best ways to avoid being an unknowing accomplice to money launderers is to properly identify new customers when their account is opened. Accordingly, the minimum identification requirements for opening a new account are listed below. If a customer refuses or is unable to provide the requested information within ten (10) business days of opening his or her account, the account should be closed.

Minimum identification requirements – Commercial accounts

1. Articles of Incorporation.
2. Board resolution authorizing the opening of the new account.
3. Letter of reference from prior bank (unless the company is newly formed).
4. Credit history for the company (unless the company is newly formed).
5. Most recent balance sheet and income statement (unless the company is newly formed; can be waived if customer has an existing relationship with the bank).
6. Last three bank statements (unless the company is newly formed; can be waived if customer has an existing relationship with the bank).
7. Identification of beneficial owners that hold over 10% of shares.

Minimum identification requirements – Consumer, business or corporation

According to the Customer Identification Program (CIP) rule, a minimum of four data items is required for all new accounts. These are:

1. Name
2. Date of birth (for an individual)
3. Address (physical home or business address, no P.O. boxes)
4. Tax Identification Number (TIN)
    a. **For individuals:** Social Security Number (SSN). For non-U.S. citizens, one of the following is acceptable:
        i. Passport number and country of issuance.
        ii. Alien identification card number.
        iii. Number and country of issuance of any other government-issued document bearing a photograph.
    b. **For businesses:** Employer Identification Number (EIN) or tax identifier for the business (TIN).

Enhanced Due Diligence – Other factors

1. New customers are expected to live or work near an office of the institution. Customers that don't meet the residency requirement will be asked to explain why they chose the particular institution. Failure to provide a sufficient explanation will be grounds for denying the account.
2. Customers that open a new account with $5,000 or more in cash will be asked to substantiate the legitimacy of the funds. If the customer can't provide sufficient proof (e.g., a payroll stub, a withdrawal receipt from another bank) the account will not be opened.
3. Customers that asked to visit their safe deposit box just prior to making deposits of $3,000 or more in a day, or $5,000 or more in a week, will be asked to substantiate the legitimacy of the funds. If the customer can't provide sufficient proof, the account will be closed.
4. Customers that asked to be excluded from CTR reporting will be reported to FinCen via a SAR. Also, their account will be closed.
5. Customers that refuse to provide the necessary information for filing a CTR will be reported to FinCen via a SAR. Also, their account will be closed.

Dollar limits for filing a SAR

The following guidelines will be used in determining when to file a SAR:

1. Suspected insider abuse – Report any amount.
2. Suspicious transactions where the institution has identified a suspect – Report if amount equals or exceeds $5,000.
3. Suspicious transactions where the institution has not identified a suspect – Report if amount equals or exceeds $25,000.
4. Known violations of the Bank Secrecy Act – Report if amount equals or exceeds $5,000. The BSA Officer will file SARs for amounts less than those specified above, if he or she has reason to believe the transaction is tied to an illegal activity.

Procedures for detecting money laundering

The institution must employ an automated system for AML detection that will enable it to detect most instances of money laundering. The BSA Officer will print and maintain reports produced by the system to substantiate his opinion that specific activity is, or is not, suspicious.

In addition to using the system, all employees will receive training once a year on how to identify money laundering operations. (New employees that have direct contact with customers will receive initial training within the first four weeks of employment.) As a part of the training, each Teller and New Accounts Representative will be given a laminated card that identifies ways to detect and prevent money laundering. Replacement cards will be available from the BSA Officer.

Identification of high-risk accounts

Certain types of businesses are more likely to be involved with money laundering. Accordingly, all businesses that are classified as one of the following will receive increased scrutiny from the BSA Officer:

1. Check cashing
2. Currency dealer or exchanger
3. Convenience stores that sell traveler's checks and/or money orders
4. Adult book stores
5. Adult entertainment clubs
6. Used car or motorcycle dealers that finance their own sales
7. Used boat dealers that finance their own sales
8. Movie theaters
9. Liquor stores
10. Apartment houses
11. Hotels

Procedures for monitoring compliance with this policy

A minimum of once a year, the institution's internal auditor or an independent third party will review the BSA Officer's suspicious activity file. The auditor will ensure that all identified suspicious activity was reviewed and appropriately handled. The auditor will also use the Cash Transaction Monitor System to search for suspicious activity that the BSA Officer may have missed.

BSA Officer training

The BSA Officer will be allowed to attend two (2) one-day training classes per year. He or she will get to choose the training. The BSA Officer will also be allowed to subscribe to a BSA newsletter service.

Sample of a Suspicious Activity Tracking Report

To (bank officer name goes here):

The following customer has been identified by the bank's compliance system as possibly being involved in suspicious activity.
Customer name:
Customer account number:

You are the loan officer, account manager or branch manager assigned to work with this customer. The Compliance Department is requesting information from you in order to conduct an investigation into this customer.

This form must be completed and returned to the bank's BSA Officer by _____.

Please answer the following questions for this customer. If necessary, you may contact the customer. However, under no circumstances are you to tell the customer his or her transaction(s) are being investigated for suspicious activity.

1. Please attach a written summary that describes the circumstances that resulted in this customer having the following transaction(s).
   –
   –
   –
   –
   –

2. Does the institution have another customer in this same business that has conducted comparable transactions?
   Yes: _____ No: _____

3. If Yes, please identify.
   Name:
   Account number:

Note: Please be advised that "willful blindness" by an officer responsible for monitoring money laundering activities is a crime under 18 U.S.C. 1956 & 1957, punishable by fines of up to $500,000 and incarceration of up to five years.

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.