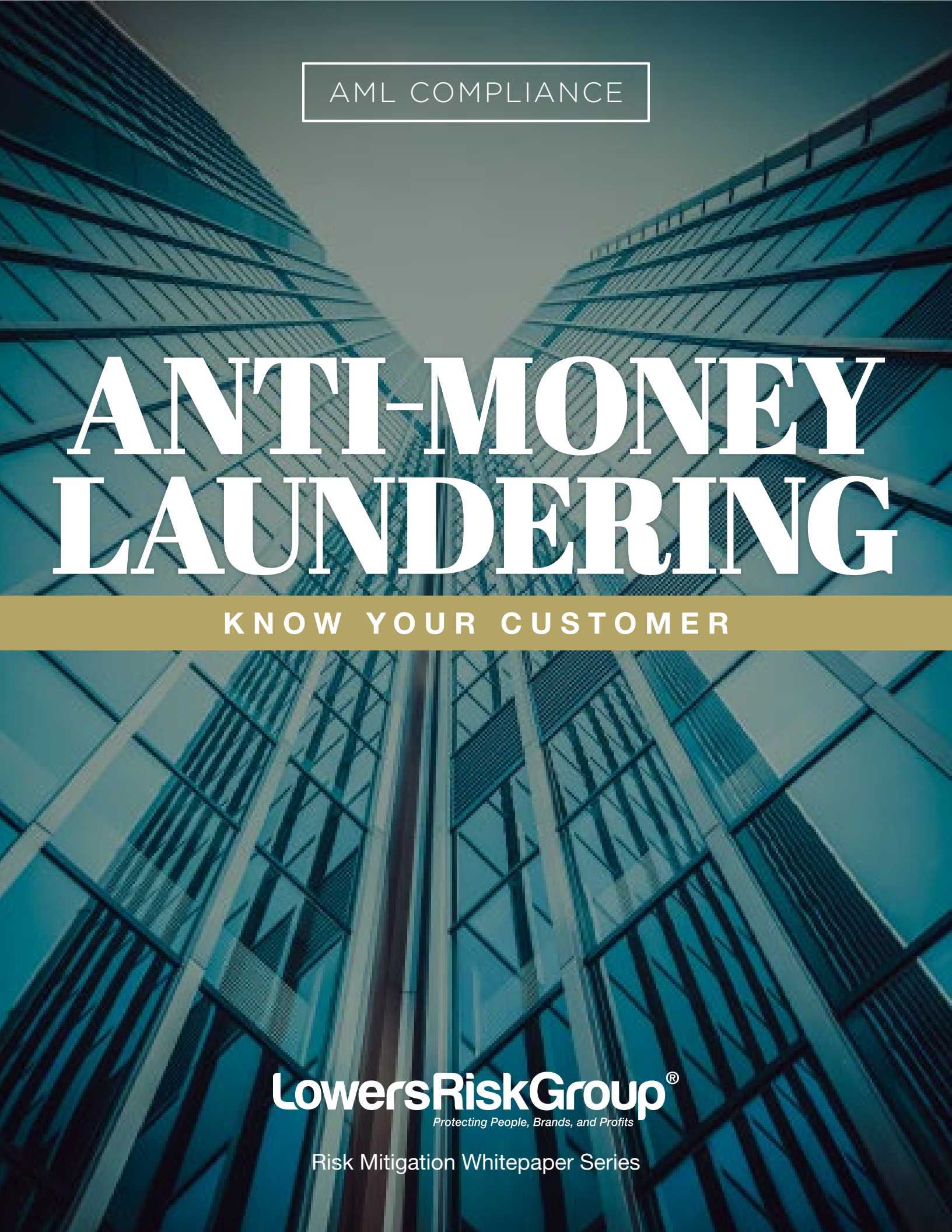


AML COMPLIANCE

ANTI-MONEY LAUNDERING

KNOW YOUR CUSTOMER

LowersRiskGroup®

Protecting People, Brands, and Profits

Risk Mitigation Whitepaper Series

EXECUTIVE SUMMARY

Money laundering is the attempt or act of concealing or disguising the nature, location, source, ownership, or control of illegally obtained money. Money laundering, in existence for centuries, is illegal and poses many risks for the legitimate business entangled in the activities of the scheme.

In simplest terms, money 'laundering' is the means by which illegally obtained proceeds (i.e., 'dirty' money) are made to appear legitimate or 'clean'. Money laundering is a crime that directly involves the criminal perpetrator and the bank, credit union, money services business, or increasingly other types of legitimate businesses that in effect facilitate the illegal money-laundering process. The process typically includes these three steps:

1 PLACEMENT

Here the illegitimately gained monies are introduced into the legitimate financial system. Traditionally, such transactions have taken place through banks either unwittingly or in complicity. However, today a wide variety of other types of legitimate non-banking businesses are being victimized by money laundering schemes.

2 LAYERING

Once introduced into the legitimate financial system, the 'dirty' money is then layered or moved around and transferred (e.g., wired) between numerous fallacious accounts. The objective of layering is to obfuscate or muddy the trail of transactions around these illegal monies.

3 INTEGRATION

Through various transactions, by moving the money between various accounts and between various financial systems, the perpetrator evades detection while slowly cleansing the dirty money until it appears legitimate or clean. Once laundered, large sums of money that might otherwise raise suspicion, can be utilized without fear of retribution.

Money laundering is nothing new. U.S. federal government attempts to safeguard the banking system from the abuses of this financial crime have been in place since at least 1970, when the Bank Secrecy Act (BSA) was enacted. The BSA established requirements for recordkeeping and reporting by private individuals, banks, and other financial institutions. It was designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the U.S. or deposited in financial institutions.

Money laundering is most commonly associated with tax avoidance, drug dealing, and terrorist activities. Such illicit activities facilitate the expansion of criminal enterprises and terror organizations as well as undermine the integrity of a financial system. Businesses and regulators alike are tasked with greater vigilance in monitoring and validating suspect financial transactions that may adversely affect commerce, the economy, or even national security.

BANK SECRECY ACT (BSA)

Since the first such legislation, the Bank Secrecy Act of 1970, also known as Title 31, numerous other laws have been passed to amend and enhance the BSA to provide law enforcement and regulatory agencies with more effective tools with which to combat the money laundering problem. These measures have afforded government agencies broader oversight, enhanced enforcement capabilities, and have granted authority to levy sanctions and fines.

These laws include the Money Laundering Control Act (1986), the Anti-Drug Abuse Act (1988), the Annunzio-Wylie Anti-Money Laundering Act (1992), the Money Laundering Suppression Act (1994), the Money Laundering & Financial Crimes Strategy Act (1998), the USA PATRIOT Act (2001), and the Intelligence Reform & Terrorism Prevention Act (2004).

BSA/AML compliance programs have been on the radar of banks, credit unions, and other types of financial institutions for years. Over the years, the administrator of the BSA, the Financial Crimes Enforcement Network (FinCEN) which is a bureau of the Treasury Department, has given authority to the Internal Revenue Service (IRS) to examine other types of businesses known as Money Services Businesses (MSBs) or Money Transfer Organizations (MTOs). These businesses include currency exchange houses, money transmitters, credit institutions, and armored car operators, as well as many non-bank businesses such as retailers, car dealers, casinos, insurance carriers and brokers, and real estate closing personnel. Most recently, digital currency and the electronic payment arms of technology companies like Facebook and Amazon are now subject to BSA/AML compliance.

Many other types of businesses, such as investment advisors, check cashers, payday loan companies, pawnbrokers, gift card operators, precious metals concerns, and marijuana sellers may also soon be subject to FinCEN oversight.

FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. According to FinCEN, an anti-money laundering program (AMLP) must be in place and working to capture and report all transactions over $10,000 by any single customer in one day or less.

Adequate record keeping, including Currency Transaction Report, multiple transaction log (designed to identify multiple, smaller transactions for the same customer that can be "rolled up" to the same threshold per day), cash exchanges log (for monitoring customer deposit/credit accounts, check cashing, foreign currency exchange), denomination exchanges (large to small, and small to large bills) for amounts greater than $1,000, and a Suspicious Activity Report applicable to any known or reasonably suspicious transactions of $5,000 or more per customer, are all part of a comprehensive AMLP review. Effective record keeping combined with thorough policies, procedures, practices, and controls review creates a strong AMLP that is the basis for effective BSA compliance.

For example, small businesses that provide money transfer (send and receive) services, also known as MTOs, are subject to the same AML guidelines as a bank or other financial institution. Similar customer identification verification and transaction record keeping rules apply across the board. Money transfer agents on both sides of the transaction must obtain and record all required customer information before a money transfer is completed. A valid form of identification must be presented by both the sender of funds and the recipient. These credentials can take the form of a driver's license, passport, or other government issued document verifying nationality or residence. If sending funds on behalf of a third party, that person's identification information must be captured as well. Typically, a person's name, address, and date of birth are gathered from the identification that is supplied. Ideally, proof of identification information should also include a photograph and the ID itself should be current.

Likewise, most sound AML transfer policies have some minimum monetary threshold (e.g., $900) for which customer identification is required for all send transactions. Further, it's important to note that requirements may vary from locale to locale in terms of minimum dollar thresholds and/or customer identification requirements. Lastly, records retention requirements pertain to all applicable transactions, regardless of the size of the organization. The period of time for which these records must be securely stored can vary, but five years is considered the best practice.

On February 23, 2012, FinCEN issued a final notice requiring the electronic filing of most BSA reports by July 1, 2012. Specifically, this action mandated the electronic submission of Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and Designation of Exempt Person Reports (DOEPs). These reports are collectively referred to hereafter as "mandated reports".

Note: **Effective April 1, 2013, financial institutions must use the new FinCEN mandated reporting, which is available only electronically through the BSA E-Filing System. FinCEN is no longer accepting legacy reports. With very limited exception, FinCEN considers financial institutions filing mandated reports in paper format to be noncompliant with the electronic filing mandate.**

All told, as the methods used by money launderers continue to evolve for banks, and as more non-bank businesses are brought under the review of BSA/AML oversight and compliance, best practices for anti-money laundering will also change. In fact, FinCEN rules can vary based on the type of organization. For example, credit card firms are not yet required to file SARs, but are required to have an AML program in place.

At the same time, the new expectation for banks and non-bank organizations alike is to 'Know Your Customer' (and in some cases, Know Your Customer's Customer), which is generally considered the best way to avoid falling prey to the evolving methods of the money launderer. These methods, of varying levels of sophistication, can include such means as imbedding mole employees within the MSB or non-banking entity (often used in gang-related activity), trade-based money laundering schemes (i.e., the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins), and moving cash in bulk (i.e., through the use of cash couriers).

A Customer Identification Program (CIP) must be included as part of every BSA/AML Compliance Program. CIP initiatives typically take the form of thorough Customer Due Diligence (CDD) investigations of vendor relationships. As for third-parties, from vendors to service providers and subcontractors, heightened expectations for risk management are based on recent outsourcing trends such as:

- **Technological advancements that have led both banks and non-bank entities to outsource subject matter expertise.**
- **The economic advantages surrounding outsourcing in general, in terms of capital and resources.**
- **Institutions/organizations outsourcing entire departments and the associated risk management functions.**

Use of third-parties may present one or more of the following risks – Operational, Compliance, Reputational, Strategic, or Credit – to the organization. To illustrate the concern, in 2013, each of the six main regulatory agencies responsible for financial institutions (i.e., the OCC, FDIC, CFPB, FFIEC, FRB, and SEC) released risk management guidance to banks for assessing and managing risks associated with third party relationships. In fact, with this guidance, the definition of 'third-party' was expanded, no longer extending to just vendors. Instead, any business arrangement between a financial institution and another entity should now be considered a third-party relationship (a financial institution's clients are exempted). Third-party subcontractor relationships are also included and are now subject to increased customer due diligence efforts.

Further, it is worth noting that whatever the nature of an organization's business/activities that are subject to BSA/AML compliance and FinCEN, a company may also need to take into account the Office of Foreign Assets Control (OFAC). The OFAC rules and regulations particularly apply when a firm is operating abroad.

OFAC administers and enforces economic and trade sanctions based upon:

- **U.S. foreign policy**
- **National security against targeted foreign countries, terrorists, and international narcotics traffickers**
- **Those engaged in activities related to the proliferation of weapons of mass destruction**

While OFAC requirements are separate and distinct from the BSA, both OFAC and the BSA share a common national security goal. For this reason, many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations; supervisory examination for BSA compliance is logically connected to the examination of a financial institution's compliance with OFAC sanctions.

WHAT YOU'LL LEARN

This white paper will expand upon the topics of BSA/AML Compliance, including the 5 main areas of an AML Compliance Program:

1. Risk Assessment
2. Internal Controls Review
3. Independent Testing (Audit)
4. BSA/AML Compliance Officer
5. BSA/AML Compliance Training

This white paper will conclude with guidance on Know Your Customer, including a look at the Customer Identification Program and Third-Party Risk Management guidelines that (in summary) include the following:

Documentation & Reporting
- Planning

Oversight & Accountability
- Due Diligence & Third-Party Selection
- Contract Review

Independent Review
- Ongoing Monitoring
- Renewal/Termination Advisory

As an organization subject to BSA/AML regulatory compliance, it is incumbent upon the board of directors, management, and staff to develop, implement, and monitor a formalized AML Program, complete with CIP, for the financial well-being of the enterprise, the markets that it operates in, the safety and security of the financial system, and of the United States, in general.

RISK ASSESSMENT

Identification of Specific Risk Categories

The first step of the risk assessment process is to identify the specific risk categories of the organization. Although attempts to launder money, finance terrorism, or conduct other illegal activities through banks, other types of financial institutions, MSBs, and non-banking businesses or organizations can emanate from many different sources, certain products, services, customers, entities, and geographic locations may be more vulnerable than others. Looking back through past incidents or losses, and being aware of industry-specific issues, one can identify those areas that have been historically abused by money launderers and criminals with greater success or frequency.

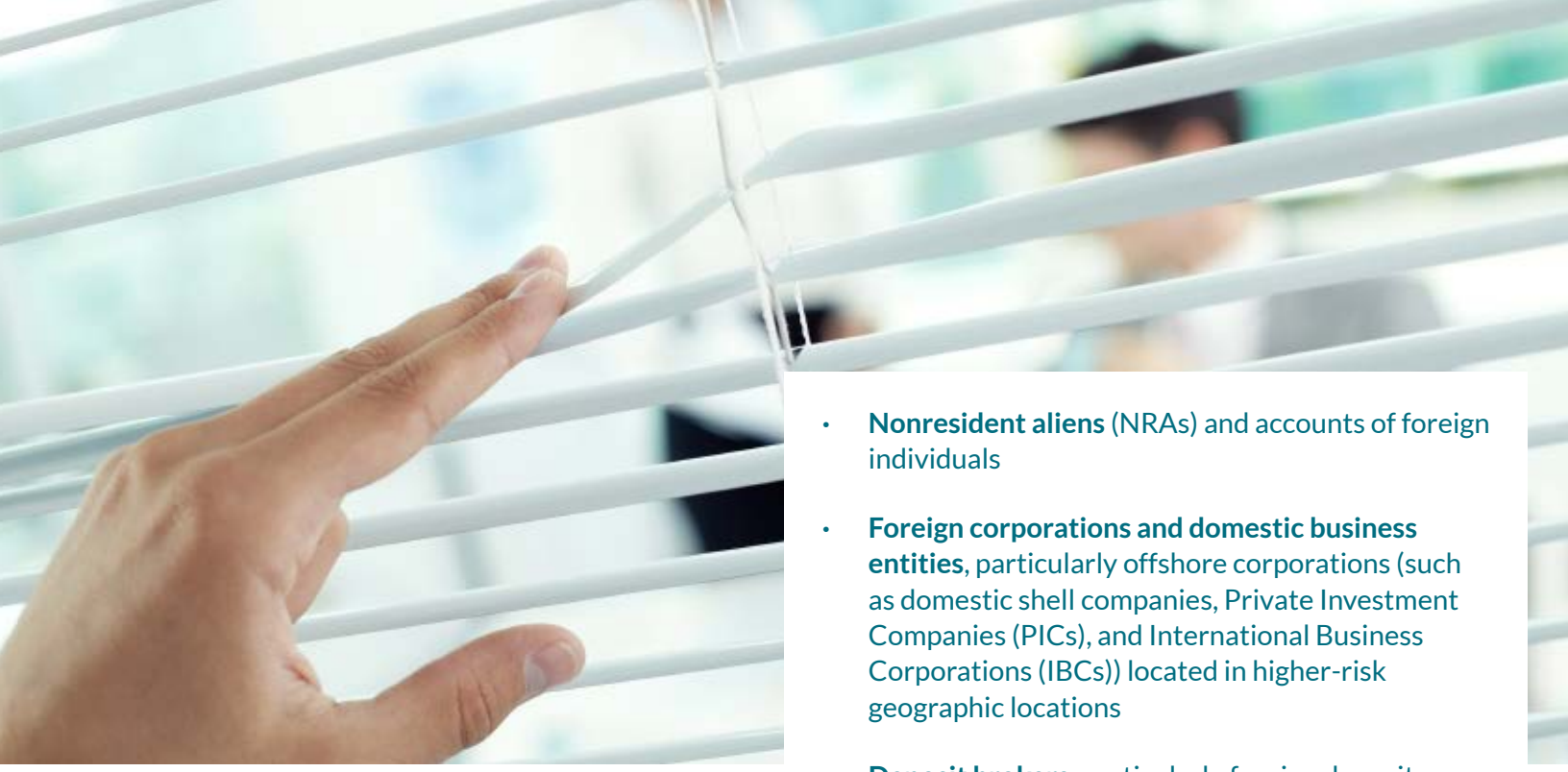
Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the type, number, and volume of transactions, and nature of the customer relationships themselves, should be considered when conducting the risk assessment. Differences in the way an organization interacts with its customers (face-to-face contact versus electronically) also should be considered. Because of these factors, risks will vary from one organization to the next. In preparing to conduct a risk assessment, the assessor should determine whether management has developed an accurate self-assessment that identifies the significant BSA/AML exposures of the organization.

The expanded sections in this white paper provide commentary on appropriate AML policies, procedures, and processes. Absent appropriate controls, these lines of business, products, or customers could elevate aggregate BSA/AML risks. The assessor should expect the organization's ongoing risk assessment process to address the varying degrees of risk associated with its products and services, customers and other entities, and geographic locations, as applicable.

PRODUCTS & SERVICES

Certain products and services offered by both banks and non-banking entities may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Examples of such products and services are listed below, although the list is by no means all inclusive:

- **Electronic funds payment services** — electronic cash (e.g., prepaid and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearing house (ACH) transactions, and automated teller machines (ATMs)
- **Electronic banking**
- **Private banking** (domestic and international)
- **Trust and asset management services**
- **Monetary instruments**
- **Foreign correspondent accounts** (e.g., bulk shipments of currency, pouch activity, payable through accounts (PTAs), and U.S. dollar drafts
- **Trade finance**
- **Services provided to third-party payment processors or senders**
- **Foreign exchange**
- **Special use or concentration accounts**
- **Lending activities**, particularly loans secured by cash collateral and marketable securities
- **Non-deposit account services** (e.g., non-deposit investment products and insurance)



CUSTOMERS & OTHER ENTITIES

Although any type of account is potentially vulnerable to money laundering or terrorist financing by the nature of their business, occupation, or anticipated transaction activity, certain customers and entities may pose specific risks. At this stage of the risk assessment process, it is essential that banks exercise judgment and neither define nor treat all members of a specific category of customer as posing the same level of risk. In assessing customer risk, banks should consider other variables, such as services sought and geographic locations. Examples of customers and entities that are especially exposed to AML risks include (but are not limited to) the following:

- **Foreign financial institutions**, including banks and foreign money services providers (e.g., casas de cambio, currency exchanges, and money transmitters)
- **Non-bank financial institutions** (e.g., money services businesses, casinos and card clubs, brokers/dealers in securities, and dealers in precious metals, stones, or jewels)
- **Senior foreign political figures and their immediate family members and close associates** (collectively known as politically exposed persons (PEPs)
- **Nonresident aliens** (NRAs) and accounts of foreign individuals
- **Foreign corporations and domestic business entities**, particularly offshore corporations (such as domestic shell companies, Private Investment Companies (PICs), and International Business Corporations (IBCs)) located in higher-risk geographic locations
- **Deposit brokers**, particularly foreign deposit brokers
- **Cash-intensive businesses** (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, and parking garages)
- **Nongovernmental organizations and charities** (foreign and domestic)
- **Professional service providers** (e.g., attorneys, accountants, doctors, or real estate brokers)

GEOGRAPHIC LOCATIONS

Identifying geographic locations that may pose a higher risk is essential to an organization's BSA/AML Compliance Program. U.S. based businesses should understand and evaluate the specific risks associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations. However, geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively.

Higher-risk geographic locations can be either international or domestic. International geographic locations of higher risk generally include:

- **Countries subject to OFAC sanctions,** including state sponsors of terrorism
- **Countries identified as supporting international terrorism** under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State
- **Jurisdictions determined to be "of primary money laundering concern"** by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act
- **Jurisdictions or countries monitored for deficiencies** in their regimes to combat money laundering and terrorist financing by international entities such as the Financial Action Task Force (FATF)
- **Major money laundering countries and jurisdictions identified** in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries which are identified as jurisdictions of primary concern
- **Offshore financial centers** (OFCs)
- **Other countries identified by the bank as higher-risk** because of its prior experiences or other factors (e.g., legal considerations, or allegations of official corruption)

Domestic higher-risk geographic locations may include, but are not limited to, banking offices doing business within, or having customers located within, a U.S. government-designated higher-risk geographic location. Domestic higher-risk geographic locations include High Intensity Drug Trafficking Areas (HIDTAs) and High Intensity Financial Crime Areas (HIFCAs).

Analysis of Specific Risk Categories

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess BSA/AML risk. This step involves evaluating data pertaining to the bank's activities (e.g., number of domestic and international funds transfers, private banking customers, foreign correspondent accounts, PTAs, and domestic and international geographic locations of the bank's business area and customer transactions) in relation to the Customer Identification Program (CIP) and Customer Due Diligence (CDD) information. The level and sophistication of analysis may vary by bank. Detailed analysis is important because within any type of product or category of customer there will be accountholders that pose varying levels of risk.

This step in the risk assessment process gives management a better understanding of the bank's risk profile in order to develop the appropriate policies, procedures, and processes to mitigate the overall risk. Specifically, the analysis of the data pertaining to the bank's activities should consider, as appropriate, the following factors:

- Purpose of the account
- Actual or anticipated activity in the account
- Nature of the customer's business/occupation
- Customer's location
- Types of products and services used by the customer

INTERNAL CONTROLS REVIEW

Internal controls are those policies, procedures, and processes designed to limit/control the risks associated with achieving compliance with AML regulations. The level of sophistication of such internal controls should be commensurate with the size, structure, risks, and complexity of the organization. It stands to reason, that larger organizations may have more personnel and resources to execute formal AML programs. In fact, larger organizations may even have the wherewithal to implement controls at the departmental level for AML compliance. That said, departmental controls can be structured to address risks and compliance requirements unique to a particular line of business or function and should be part of a comprehensive AML compliance program.

Smaller organizations may have a more difficult task marshalling the internal resources, working out the segregation of duties, and (where necessary) assigning the dual control responsibilities that are ideal for achieving compliance. Nonetheless, with the appropriate planning and guidance, smaller organizations can meet their obligations for AML compliance without overtaxing resources or exceeding a budget.

Regardless of an organization's size, a sound approach to internal controls relative to an AML compliance program should be implemented and should include (but should not be limited to) the following tasks:

- **Identify those products, services, customers, third-parties, and locations that are more vulnerable to abuse by money launderers.**
- **Determine who should be tasked with managing AML compliance initiatives**, including identifying compliance deficiencies and any corrective actions taken. Oftentimes, an AML committee is assigned or formed specifically for this purpose. Whether an AML officer, committee, and/or other approaches are taken, those person(s) should also be responsible for keeping the Board of Directors and senior management informed.
- **Provide for AML program continuity** despite any changes in the Board, senior management, AML committee, or key employee involvement over time.
- **Implement risk-based Customer Due Diligence** (CDD) policies, procedures, and processes.
- **Identify reportable transactions, accurately file all required reports, and have a system** (manual or automated) in place for the processing of all Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and CTR exemptions.
- **Provide for dual controls and the segregation of duties to the extent possible.** For example, employees that complete the reporting forms (such as SARs, CTRs, and CTR exemptions) generally should not also be responsible for the decision to file the reports or grant the exemptions.

Train all employees to be aware of their responsibilities under the AML regulations and internal policy guidelines. For those directly involved in the AML compliance program, incorporate their responsibilities directly into their job descriptions and/or performance evaluations, as appropriate.

- **Provide for adequate supervision of all employees** that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by AML guidelines and associated regulations.
- **Meet all regulatory recordkeeping and reporting requirements**, evaluate all recommendations for improved AML compliance, and provide for timely updates in response to any changes in regulations.

Ultimately, the Board of Directors, acting through senior management, is responsible for ensuring that the organization's AML internal controls, monitoring, and reporting infrastructure are adequate and maintained. As is often suggested in discussions around crime and fidelity related risk mitigation, the board of directors and senior management are responsible for creating a "culture of compliance" to ensure that staff remain vigilant and adhere to organizational AML policies, procedures, and processes.

INDEPENDENT TESTING (AUDIT)

Testing or audit of the policies, procedures, and processes that comprise an organization's AML Program should be periodically conducted on both an internal and external basis. The Internal Audit staff or department is the most likely resource to be tasked with the internal evaluation of AML practices. Of course, qualified personnel who are involved with internal audits should not be involved in the function being tested. Further, such efforts should be ongoing and complement the periodic external testing/auditing of an independent auditor, consultant, or other qualified party.

External testing should be conducted by a reputable independent third-party auditor. While the frequency of such external audits is not specifically defined in any regulation, outside audits conducted every 12 to 18 months should be commensurate with the risk profile of almost any organization that is subject to AML oversight. Of course, financial institutions are more likely to be audited on a shorter cycle than other types of organizations.

Further, those persons responsible for conducting an independent evaluation of the written AML compliance program should perform testing for specific compliance with the BSA (and/or other applicable laws) and evaluate pertinent management information systems (MISs). All audits should be risk based and evaluate the quality of risk management for all operations, departments, and subsidiaries. Risk-based audit programs will vary depending on the organization's size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. An effective risk-based auditing program will cover all of the organization's products, services, and activities. The frequency and depth of each activity's audit will vary according to the activity's risk assessment. Risk-based auditing enables the board of directors and auditors to use the organization's risk assessment to focus the audit scope on the areas of greatest concern. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

INDEPENDENT TESTING SHOULD, AT A MINIMUM, INCLUDE:

- **An evaluation of the overall adequacy and effectiveness of the AML compliance program,** including policies, procedures, and processes. Typically, this evaluation will include an explicit statement about the program's overall adequacy, effectiveness, and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (e.g., an examiner, review auditor, AML officer, or board/committee member) to reach a conclusion about the overall quality of the program
- **A review of the organization's risk assessment for reasonableness given its risk profile** (products, services, customers, entities, and geographic locations)
- **Appropriate risk-based transaction testing to verify the organization's adherence to the AML recordkeeping and reporting requirements** (e.g., CIP, SARs, CTRs, CTR exemptions, and information sharing requests)
- **An evaluation of management's efforts to resolve any violations and/or deficiencies noted in previous audits** (and for banks, regulatory examinations) including progress in addressing outstanding supervisory actions, if applicable
- **A review of staff training** for adequacy, accuracy, and completeness
- **A review of the effectiveness of any systems used for suspicious activity monitoring** (manual, automated, or a combination). Related reports may include, but are not limited to:

  - Suspicious activity monitoring reports
  - Large currency aggregation reports
  - Monetary instrument records
  - Funds transfer records
  - Nonsufficient funds (NSF) reports
  - **Large balance fluctuation reports**
  - **Account relationship reports**
- **An assessment of the overall process for identifying and reporting suspicious activity,** including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness
- **An assessment of the integrity and accuracy of information systems used in the AML compliance program.** For example, this includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports

---

Auditors should document the audit scope, procedures performed, transaction testing completed, and findings of the review. Any violations, policy or procedures exceptions, or other deficiencies noted during the audit should be included in an audit report. For banks, all audit documentation and work papers should be made available for examiner review upon request.

Lastly, both the internal and external parties tasked with the audit function should report their findings directly to the board of directors or a designated board committee comprised primarily or completely of outside directors. Working on behalf of the board or committee, management should work with audit personnel to track audit deficiencies and document corrective actions.

BSA/AML COMPLIANCE OFFICER

The board of directors of an organization must designate a qualified individual to serve as the BSA/AML Compliance Officer. This person is responsible for coordinating and monitoring the day-to-day AML compliance activities of the organization. This person is charged with managing all aspects of the AML compliance program and with managing the organization's adherence to the BSA and its implementing regulations. Note however, the board of directors bears ultimate responsibility for the organization's overall AML compliance.

While the title of the individual responsible for AML compliance is not important, his/her level of authority and responsibility is critical. The AML Compliance Officer may delegate duties to other employees, but the officer should be responsible for overall compliance. The board of directors is responsible for ensuring that the compliance officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective compliance program based on the organization's risk profile.

The AML Compliance Officer should be fully knowledgeable of the BSA and all related regulations. The compliance officer should also understand the organization's products, services, customers, entities, geographic locations, and the potential for money laundering and terrorist financing risks associated with those activities. The appointment of a compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or time to satisfactorily complete the job.

The line of communication should allow the compliance officer to regularly apprise the board of directors and senior management of ongoing compliance with the BSA. Pertinent AML-related information, including the reporting of SARs filed with FinCEN, should be reported to the board of directors and/or an AML board committee so that these individuals can make informed decisions about overall compliance. The compliance officer is responsible for carrying out the direction of the board and ensuring that employees adhere to the organization's AML policies, procedures, and processes.

BSA/AML COMPLIANCE TRAINING

All organizations subject to BSA/AML compliance must ensure that the appropriate personnel are trained in the applicable aspects of AML compliance. The training should take into account all applicable regulatory requirements and the internal AML policies, procedures, and processes of the organization. The training efforts or program should include (but not necessarily be limited to) the following:

APPLICABLE PERSONNEL

At a minimum, the training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person's specific responsibilities. Such training should include an overview of the BSA/AML requirements for all new staff as part of their orientation. Periodic ongoing training (annually, at a minimum) should take place for all existing employees. Refresher training should focus on any changes in regulations and the respective compliance initiatives, with emphasis on those business lines that are susceptible to money laundering activities.

BSA/AML COMPLIANCE OFFICER

Training for the person designated as AML Compliance Officer should be given special consideration. As such, they should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall BSA/AML risk profile of the organization.

BOARD OF DIRECTORS AND SENIOR MANAGEMENT

Given their role in establishing a "culture of compliance", the board of directors and senior management must be kept informed of all relevant changes and new developments in the training efforts or program. While the board may not require the same degree of training as others in the organization, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the organization. Without a general understanding of what's taking place on the BSA/AML front, the board cannot adequately provide oversight; approve new policies, procedures, and processes; or provide sufficient resources for training and compliance efforts.

TABLE TOP EXERCISES

If possible, examples of money laundering activity, including suspicious activity monitoring and reporting should be made part of the training effort with examples and table top exercises. For example, in banks, training for tellers should focus on examples involving large currency transactions or other suspicious activities; training for the loan department should provide examples involving money laundering through lending arrangements.

TRAINING DOCUMENTATION

Organizations should document their training efforts/programs. Training materials, dates of training sessions, and attendance records should be maintained by the AML Compliance Officer and be made available for review by examiners upon request.

KNOW YOUR CUSTOMER (KYC)

A Closer Look at Customer Identification Programs (CIPs) and Third-Party Risk Management Guidelines

As indicated above, varying degrees of risk are associated with the products and services, customers and other entities, and geographic locations in various types of organizations. Depending upon these variables, as well as the nature of business being conducted and the size and type of organization, Know Your Customer (KYC) guidelines can vary quite broadly.

In addition to verifying proof of identity and conducting related due diligence, understanding the monetary thresholds and rules required for reporting, gathering the appropriate information for recordkeeping on applicable transactions, and adhering to record retention requirements, specific FinCEN (or other) rules apply concerning:

1 HIGH CURRENCY AMOUNT TRANSACTION REPORTING

This applies for individual or multiple transactions that exceed a specific monetary threshold, and may be required over different periods of time, especially if knowledge exists that the transactions are being conducted by or on behalf of the same person.

2 STRUCTURING

As indicated earlier, structuring is the act of breaking up a potential large transaction into several smaller transactions. It is illegal to assist your customers (or third-parties on whose behalf they are acting) to structure transactions in order to avoid record keeping or large transaction reporting requirements.

3 SUSPICIOUS ACTIVITY/ TRANSACTION REPORTING

Many factors are involved in determining whether transactions are suspicious including the amount, the location of your organization, where the transactions are being sent, from where the transactions are being received, as well as other AML concerns that may exist based on location, comments made by the customer, the customer's behavior, etc. Suspicious Activity/Transaction Reporting is required for any transaction or pattern of transactions that is/are attempted or conducted for any amount for which one knows, suspects, or has reason to suspect that the involved funds:

- **Are derived from illegal activity or there is intent to hide funds obtained from illegal activity;**
- **Are structured to avoid recordkeeping or reporting requirements;**
- **Have no business or apparent lawful purpose;**
- **Facilitate criminal activity.**

4 FRAUD PREVENTION

According to the Association of Certified Fraud Examiners (ACFE), businesses lose an estimated 5% of revenues each year to fraud. If applied to the 2013 estimated Gross World Product, this translates to a potential projected global fraud loss of nearly $3.7 trillion.

5 TERRORISM FINANCING PREVENTION

The Financial Action Task Force (FATF), an inter-governmental body developing and promoting policies to combat money laundering and terrorist financing, along with FinCEN, have both issued guidance on financial transactions that may be indicative of terrorist financing. This guidance applies to banks, other depository institutions, and MSBs alike and includes such activities as:

- **The movement of funds either through a country designated by FATF or FinCEN as "non-cooperative" by a person who is identified as a specially designated national by OFAC (see below) or a person who appears on the United Nation's list of blocked accounts;**
- **Multiple transactions conducted by a group of nationals from countries associated with terrorist activity;**
- **Individuals acting on behalf of a MSB or MTO that use the organization to transfer funds to multiple locations as this may be indicative of an unlicensed operator seeking to evade the banking system to conduct foreign transfers.**

6 INTERNATIONAL GOVERNMENT WATCH LISTS

As indicated above, especially with respect to criminal and terrorist activity, many countries maintain and publish watch lists that are designed as a reference tool for businesses to assist in complying with the sanctions programs of various governmental bodies such as the U.S. Treasury's Office of Foreign Assets Control (OFAC), Interpol Most Wanted, European Union Terrorist, Australia Consolidated, and Canadian Consolidated lists. Each country's watch list prohibits businesses and other types of organizations from conducting any form of activity with any of the entities or persons that are on these lists. In the U.S., OFAC's list is commonly referred to as the Specially Designated Nationals (SDN) list.

WHAT TO DO?

So, what's a business or organization that is subject to AML regulations to do with regard to KYC? To answer this question, let's take a closer look at Customer Identification Programs (CIPs) and Third-Party Risk Management guidelines.

CUSTOMER IDENTIFICATION PROGRAMS (CIP)

PLANNING, DOCUMENTATION & REPORTING:

All banks and most other types of financial institutions must have a written CIP. For banks, the CIP rule of the USA PATRIOT Act requires the bank to implement a written CIP that is commensurate with its size and type, and one that includes certain minimum requirements (see Minimum Requirements below). The CIP must be incorporated into the bank's BSA/AML compliance program, which is subject to the approval of the bank's board of directors. The implementation of a CIP by subsidiaries of banks is appropriate as a matter of safety and soundness and protection from reputational risks. Although not covered here, rules can vary further between domestic and foreign subsidiaries of the bank.

As indicated earlier, beyond banks and other financial institutions, many other industries and types of organizations are subject to BSA/AML regulation and the CIP rules surrounding their interactions with customers. In short, the CIP is intended to enable the organization to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. In fact, those organizations required to develop a CIP should also conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider:

- **The types of accounts being offered;**
- **The policies and procedures for opening accounts;**
- **The types of customer identifying information being sought in order to open an account; and**
- **The organization's size, location, and customer base,** including types of products and services used by customers in different geographic locations.

Pursuant to the CIP rule, an "account" is defined as a formal customer relationship to provide or engage in services, dealings, or other financial transactions, and typically includes a deposit account, a transaction or asset account, a credit account, or another extension of credit. An account also includes a relationship established to provide a safe deposit box or other safekeeping services or to provide cash management, custodian, or trust services. With that said, an account does not include:

- **Products or services for which a formal business relationship is not established with a person**, such as check cashing, funds transfer, or the sale of a check or money order;
- **Any account that the organization acquires.** This may include single or multiple accounts as a result of the purchase of assets, acquisition, merger, or assumption of liabilities;
- **Accounts opened to participate in an employee benefit plan** established under the Employee Retirement Income Security Act (ERISA) of 1974.

To recap, the CIP rule applies to a "customer." A customer is a "person" (an individual or a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a new account, a person who opens a new account for another person who lacks legal capacity, or a person who opens a new account for an entity that is not a legal person (e.g., a civic club).

For example, in a banking environment, a customer does not include a person who does not receive banking services, such as a person whose loan application is denied. The definition of "customer" also does not include an existing customer as long as the bank or organization has a reasonable belief that it knows the customer's true identity. Excluded from the definition of customer are federally regulated banks, banks regulated by a state bank regulator, governmental entities, and publicly traded companies.

Lastly, when gathering applicable customer information, the organization must have policies and procedures in place for establishing, maintaining, and safeguarding the customer records as they pertain to BSA/AML guidelines. Most organizations already have some form of accounting or CRM technology in place to manage customer accounts and related information. The key to a CIP is to gather the right amount of the right information so as to fully comply with AML compliance program requirements and at the same time not put the organization at undue risk by having accumulated too much or irrelevant information on its customers. Having the correct amount and type of customer information in place better facilitates the oversight and accountability required by the organization in conducting its due diligence investigations and third-party risk management oversight.

OVERSIGHT & ACCOUNTABILITY:

Effective oversight and accountability of customer due diligence activities, including the selection and management of third-party providers, is paramount. The organization should seek out reputable provider(s) then scrutinize the terms of contract, the methods used, and applicable fees associated with conducting customer investigations. Such investigations may include any/all of the following:

- **Public Records Research**
- **Corporate & Personal Criminal Background Checks**
- **Asset Search Tracking (both corporate and individual)**
- **Law Enforcement Inquiries**
- **On-Site Investigations**

For example, for an individual, due diligence activities will be carried out using a variety of resources, both public and proprietary. They will include (but are not limited to) the following areas of investigation:

PUBLIC RECORDS

A thorough review of publicly available records pertaining to the individual or subject of the investigation. This review of public records is based on informational database searches on the known name/alias of the subject. The results of this search will confirm (or may potentially conflict with) the information supplied on the customer application. Such searches may identify the following:

- **Full name** (including middle initial and suffix, if applicable), maiden/previous name, alias, or other known names or persona(s)
- **Date of birth or approximate age**
- **Social Security** (truncated) or other ID numbers (e.g., driver's license, passport, identification card, etc.)
- **Current and previous addresses** or, if not available, general geographic area(s) of current/past residence(s) and/or place(s) of employment
- **Current employer and employment history** (if available)

CORPORATE & PERSONAL CRIMINAL BACKGROUND CHECKS

With customer pre-approval, and typically conducted through a licensed Credit Reporting Agency (CRA), criminal background checks tap various commercial and proprietary databases that may supply additional customer-related identifiable information, such as:

- **Corporate registration(s)** under the subject's name
- **Preliminary information on warrants or criminal record** and/or civil actions, tax liens, or judgments
- **Any known or suspected affiliation with illicit or criminal organizations**
- **Any other information about the subject that the organization feels is relevant** and pertinent to the KYC investigative effort

ASSET TRACKING SEARCHES

Asset Tracking Searches comprise an investigation of local, regional, and (if necessary) national informational resources as well as other publically available sources of related asset information. Such research typically includes (but is not limited to) the following:

- **Real property ownership**
- **Vehicle/boat ownership**
- **Other property ownership** (e.g., second home, rental property)
- **Business ownership or minority/majority interest**, as applicable

All asset checks include reference to the government databases, local courts, and other sources such as the real estate property offices.

LAW ENFORCEMENT

Inquiries with local, state, regional, and/or national law enforcement, as necessary and approved, to uncover any prior convictions or pending criminal proceedings.

ON-SITE INVESTIGATIONS

Conduct on-site investigations of the applicable subject on an as needed basis or where electronic database searches have yielded little, if any, useful information.

INDEPENDENT REVIEW:

In terms of ongoing monitoring, part and parcel with the independent audit of any AML program (and respective CIP) is a thorough review and understanding of controls that are in place within the organization's operations and related cash management activities. Here, the auditor is looking to see that reportable transactions are being properly identified, to ensure that all necessary reports are being completed and filed in a timely fashion, to verify that the organization employs adequate supervision of all employees subject to AML guidelines, and to ensure that dual controls and segregation of duties are taking place, especially with respect to the recording/filing of all reports.

In addition, independent review will evaluate how customer renewal and/or termination policies, procedures, and practices are carried out within the organization.

In summary, at a minimum, an organization's CIP must include the following:

1 INFORMATION REQUIRED OF CUSTOMERS

A description of the types of identifying information the organization will obtain from customers opening new accounts.

2 CUSTOMER VERIFICATION

Procedures for verifying the identifying information provided, to the extent reasonable and practical, within a reasonable period of time before or after a new account is opened. This verification process may take any of the following forms:

- **Verification through various documents** provided by the customer or other sources
- **Verification through non-documentation methods** or sources (e.g., reliance on other financial institutions and/or the use of third-parties)
- **Additional verification measures** for certain customers
- **Lack of verification** - See point 6 below

3 RECORD KEEPING / RETENTION

Procedures for establishing / maintaining customer records pertaining to the CIP.

4 COMPARISON OF CUSTOMER INFORMATION TO GOVERNMENT WATCH LISTS

Procedures for determining whether customers opening new accounts appear on any government watch lists as designated by OFAC, FinCEN, FATF, SEC or other applicable governing body.

5 THE PROVIDING OF ADEQUATE NOTICE TO THE CUSTOMER

Procedure for providing notice to customers prior to account opening that information may be requested to verify their identity.

6 LACK OF VERIFICATION

Procedures specifying the action(s) the organization will take when it cannot adequately verify the identity of the individual or entity opening a new account.

7 OTHER LEGAL REQUIREMENTS

Ensure that any other legal requirements may be met with regard to the CIP, for example any state/local or industry-specific regulatory guidelines that must legally be met. In addition, ancillary items such as contract negotiations with third-parties for due

diligence work, independent audit, and any ongoing oversight work. Lastly, when the organization cannot adequately verify a prospective customer, policies and procedures must be in place for renewing or terminating arrangements with third-parties and/or customer relationships.

THIRD-PARTY RISK MANAGEMENT CONSIDERATIONS

Almost every type of organization has third-party relationships to manage. Use of third-parties may present one or more of the following risks -- Operational, Compliance, Reputational, Strategic, or Credit -- to the organization. As cited earlier in this paper, from service providers to subcontractors, heightened expectations for sound risk management and effective contract review are based on recent trends in outsourcing.

FinCEN (and any of a number of other regulatory agencies) expanded the definition of 'third-party' in the banking industry to include any business arrangement between a financial institution and another entity. Even though a financial institution's clients are exempted, third-party subcontractor relationships are included and are now subject to increased CDD efforts.

Lastly, as also alluded to earlier, whenever an organization's activities take it abroad and international third-party relationships come into the equation, one must also take into account OFAC rules and regulations. OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

Therefore, prudent third-party risk management considerations should be given serious consideration in every organization. For banks and other financial types of institutions in particular, due diligence efforts should include the gathering of information from a comprehensive list of items prior to deciding to enter into a contract with a third-party, including (but not necessarily limited to) the following:

- **Strategic Goals**
- **Legal & Regulatory Compliance**
- **Financial Condition**
- **Business Experience & Reputation**
- **Fee Structure & Incentives**
- **Qualifications & Background of the Third-Party's Principals**
- **Risk Management Practices**
- **Information Security Program**
- **Resilience**
- **Incident Reporting & Management Programs**
- **Physical Security**
- **Human Resource Management**
- **Subcontractor Reliance**
- **Insurance Coverage**
- **Conflicting Contractual Relationships (that may cause risk to the bank)**

Then, pending the approval of any given vendor or subcontractor relationship, the organization is tasked with a bevy of contractual negotiations that must be met for both new and existing agreements. Contract templates require ongoing updates:

- **Nature & Scope of the Arrangement**
- **Performance Measures or Service Level Agreements**
- **Responsibilities for Providing, Receiving, or Maintaining Information**
- **Right to Audit & Require Remediation**
- **Responsibility for Compliance with Applicable Laws and Regulations**
- **Cost & Compensation**
- **Ownership & License**
- **Confidentiality**
- **Business Resumption & Contingency Plans**
- **Indemnification**
- **Insurance**
- **Dispute Resolution**
- **Limits of Liability**
- **Default & Termination**
- **Customer Complaints**
- **Subcontracting**
- **Foreign-Based Third-Parties**
- **Acknowledgement of Regulatory Supervision**

Last but not least, the ongoing monitoring of the third-party relationship(s) that an organization enters into is an essential component of the risk management process which should include (at a minimum) the following:

- **A determination of the appropriate level of monitoring based on risk**
- **A schedule of vendor site visits that may provide an opportunity to assess risk and/or evaluate controls, and to verify responses to due diligence items**
- **The implementing of periodic "checkpoints" to discuss vendor performance, complaints, or other issues**

All of that said, the impact of such sweeping change in the realm of third-party relationships, in large part due to the added regulatory environment in which banks and other types of organizations now operate, depends on which side of the fence you're standing. The impact to banks, financial institutions, and other types of organizations subject to AML due diligence guidelines is as follows:

- **Regulatory requirements have become more stringent**
- **Additional oversight coming from [multiple] regulators**
- **Self-policing & self-reporting may be a thing of the past**
- **Remediation efforts are looked at more closely**
- **Clear potential for a reduction in third-party relationships**

From the perspective of the third-party, the potential impacts are monumental as well to include (but are not limited to) the following:

- **Heightened standards by banks, financial institutions, and more non-bank organizations**
- **More audits, more meetings**
- **Consumer complaints and issues to be reported and tracked**
- **Revised contracts**
- **Economics may not justify the cost**

For banks especially, enforcement actions brought government bureaus such as the OCC and CFPB, and pertaining to non-compliance, can run into the millions of dollars, including both restitution and civil penalties.

In conclusion, third-party risk management is a "hot topic" and is one that is not going away any time soon. Best practices and "take-aways" for the banks, financial institutions, and non-banking entities subject to AML regulation, as well as their vendor and sub-contractor partners, include the following:

- **Understand the new requirements and regulatory bodies to whom you must answer. This can vary widely depending upon your organization and the industry in which you operate.**
- **Conduct a self-assessment to help proactively identify gaps.**
- **Document your practices, relationships, and risk oversight activities.**
- **Leverage the awareness of and increased responsiveness to these requirements as a competitive advantage.**

Source:

U.S. Department of the Treasury

FinCEN: History of Anti-Money Laundering Laws

CASE STUDY #1

FinCEN Fines Former Casino Staffer Over AML Lapses

The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) fined a former casino staffer over anti-money laundering violations and barred him from working at financial institutions. FinCEN fined the former VIP services manager at a casino, $5,000 and said he helped high-end gamblers avoid detection of large cash transactions by agreeing not to file suspicious activity reports or currency transaction reports.

During a criminal investigation the manager assured an undercover agent, posing as the representative of a Russian businessman, that the casino wouldn't file reports if his client brought large amounts of currency to the casino, FinCEN said.

The manager was also criminally charged last year for failing to file a currency transaction report. He entered into a deferred prosecution agreement in June and agreed to cooperate with investigators as a part of that agreement, according to court documents.

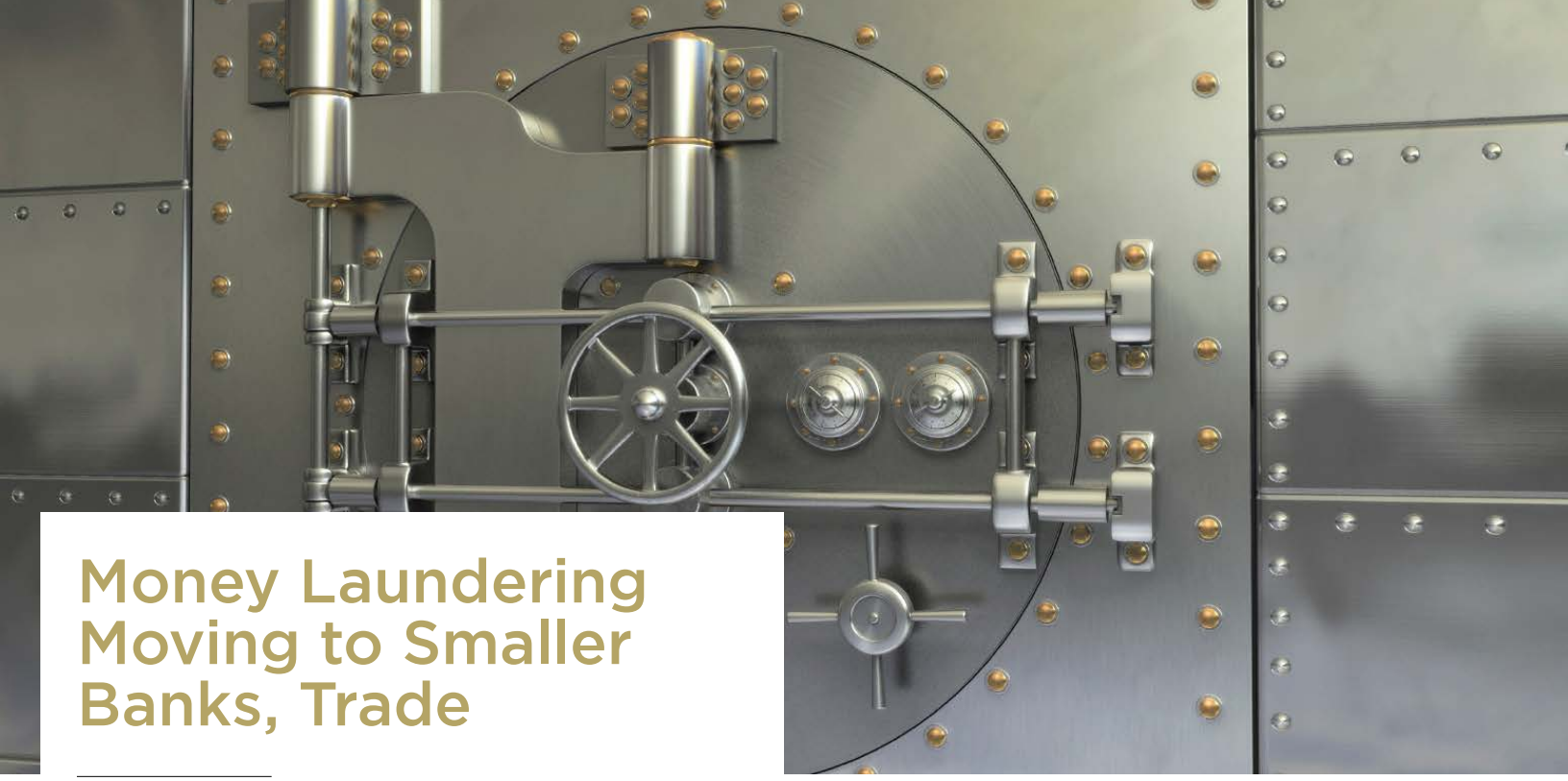
The agency has signaled that it will pursue cases like this. Officials have said it plans to focus on both the casino industry and penalizing individuals.

FinCEN said it continues to investigate the activities of the casino.

Source:

The Wall Street Journal, August 21, 2014

CASE STUDY #2



Money Laundering Moving to Smaller Banks, Trade

Money launderers are increasingly looking for ways to avoid tight controls at major banks, including embedding moles within smaller banks and engaging in more trade-based schemes, law enforcement officials said at a Las Vegas anti-money laundering conference on Monday.

"We are seeing the movement of [illicit] money into [smaller community] banks as well as even the implanting of personnel who are getting jobs at those banks who can work for them on the inside," said Bryan Smith, unit chief of the financial crimes section of the Federal Bureau of Investigation's criminal investigative division.

"It's one of those things where you tighten the screws in one area and then it pushes [the criminals] somewhere else and then they find some loopholes there," he said at the event, run by the Association of Certified Anti-Money Laundering Specialists.

Angela Byers, the section chief of the financial crimes section of the FBI's criminal investigative division, said that tighter controls at banks have also led to an increase in trade-based money laundering. "Trade-based money laundering schemes are not new, but we believe they are becoming more prevalent as it becomes harder to use the banking system to move money," said Ms. Byers.

Criminals also turn to moving cash in bulk when banks have tight controls, stated Joseph Burke, unit chief of Homeland Security Investigations' National Bulk Cash Smuggling Center. "If you all don't do your job, I go out of business because there would be no need to move money via bulk cash," he told the audience of anti-money laundering professionals.

Source:

The Wall Street Journal, September 29, 2014

CASE STUDY #3

FinCEN Warns Banks on Axing Customers

Regulatory scrutiny has led banks to close money-services business accounts in recent years. But now one regulator is suggesting that banks might need to rethink that approach.

The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) on Monday urged banks to use caution when broadly cutting the accounts of money-services businesses, or MSBs, which can face a higher risk of money laundering.

"FinCEN does not support the wholesale termination of MSB accounts without regard to the risks presented or the bank's ability to manage the risk," the agency said in a statement meant to "reiterate expectations" for banks. "MSBs represent varying degrees of risk, and not all money-services businesses are high-risk."

As U.S. authorities have stepped up scrutiny of banks' anti-money laundering controls in recent years, many banks have started to shy away from MSB customers, which include money transmitters and check-cashing firms.

These MSBs and similar firms can face a higher risk of money laundering for a number of reasons, including a lack of ongoing customer relationships, an official anti-money laundering manual says. Banks are turning away from the businesses in part because they don't want to take on the potential money-laundering risk posed by having the firms as customers.

Barclays PLC, for instance, has said it moved last year to close the accounts of about 250 MSBs, which accounted for about 75% of all MSB customers. This decision generated controversy because one of these accounts belonged to Somali money transfer firm Dahabshiil, which fought the closure. Barclays and Dahabshiil earlier this year said the money transfer firm's account would be closed as part of a settlement.

Some in the industry, including a former head of FinCEN, have expressed concern that closing potentially higher-risk accounts could backfire on banks. For one, the move could drive dirty money underground where authorities could have a more difficult time monitoring it. The agency nodded to this concern in its statement.

> "Refusing financial services to an entire segment of the industry can lead to an overall reduction in financial sector transparency that is critical to making the sector resistant to the efforts of illicit actors," FinCEN said.

Source:

The Wall Street Journal, November 10, 2014

ABOUT LOWERS RISK GROUP

Lowers Risk Group (LRG) combines the services of three industry-leading companies: Lowers & Associates, Proforma Screening Solutions, and Wholesale Screening Solutions – to create a complete risk management service offering for organizations of all types and sizes. Employed in concert or on a standalone basis, LRG excels in providing comprehensive enterprise risk management (ERM) and human capital risk management (HCRM) solutions to organizations operating in high-risk and/or highly-regulated environments. Our specialized background screening and crime and fidelity related risk mitigation services protect people, brands, and profits from avoidable loss and harm. With Lowers Risk Group you can expect a discreet, experienced, and professional approach to your risk assessment, compliance, human capital, and risk mitigation needs to help move your organization forward with confidence.

LowersRiskGroup®

Protecting People, Brands, and Profits

LowersRiskGroup.com 540-338-7151

125 East Hirst Road, Suite 3C,
Purcellville, VA 20132