THE UNDERBELLY OF AML DE-RISKING:
EXECUTING CASE-BY-CASE ACCOUNT CLOSURE DECISIONS

April, 2015 | Iris Smith, CAMS-Audit

ACAMS® Advancing Financial Crime Professionals Worldwide
# Table of Contents

- **Executive Summary** .......................................................................................... 3
- **Conflicting Messages** ......................................................................................... 4
  - Regulatory Guidance .............................................................................................. 4
- **The Three E’s of De-Risking** .............................................................................. 6
  - Establish Risk Appetite ........................................................................................... 6
  - Execute a Consistent, Repeatable and Auditable Process ..................................... 7
    - Well-Documented Process ....................................................................................... 8
    - Auditability ........................................................................................................... 10
  - Educate Relationship Managers ........................................................................... 11
- **Law Enforcement Requests** ............................................................................... 11
- **Managing Disagreements** .................................................................................. 12
  - BSA/AML Penalty Cases ......................................................................................... 12
- **Enduring Challenges** ........................................................................................ 13
  - Connecting Relationship Dots ............................................................................... 13
  - Relationships that are Impossible to Terminate ................................................... 13
  - Continued Surveillance (Prohibited Customer List) ............................................. 14
- **Final Comments** ................................................................................................ 15
  - Unintended Consequences .................................................................................... 15
- **Works Cited** ....................................................................................................... 16
  - Resource ............................................................................................................... 17
Executive Summary

Regardless of a financial institution’s size, complexity and regulatory authority, each institution faces account closure decisions when the money laundering (ML) or terrorist financing (TF) risk of keeping a customer relationship outweighs the cost/benefit of the relationship, more recently referred to as ‘de-risking.’ Differences between financial institutions regarding the actual execution of account closures appear when you compare risk appetite between those institutions. What might be considered medium risk for one institution may be considered high risk for another.

Determining risk appetite is often contingent on the types/classes of customers institutions are interested in establishing and maintaining. For example, an institution may decide not to provide services to international money services businesses (MSBs) for various reasons such as the inherent risk exposure, increased AML monitoring expectations and the overall cost of risk mitigation. On the other hand, FinCEN Director Jennifer Shasky Calvery recently urged financial institutions to not refuse financial services to an entire segment of the industry (i.e., MSBs) due to a fear of compromising transparency of the financial sector and making the sector resistant to the efforts of illicit actors (Calvery, 2014).

No prescription or formula exists to instruct institutions on how and when to discontinue risky customer relationships. However, regulatory expectations to effectively manage high-risk financial activities are ever present as evidenced by continual enforcement actions against financial institutions for Bank Secrecy Act (BSA) violations and compliance program failures.

While the concept of de-risking is centered on institutions who are ‘wholesale’ de-risking or getting rid of entire classes of customers because of risk, this paper will focus on the challenges that exist when financial institutions execute on a case-by-case basis. Exiting a single account or an entire customer relationship is complex, costly and for most institutions, extremely difficult to manage in a consistent and effective manner.

Although financial institutions are not required to maintain a particular customer relationship, ultimately the decision to close an account or restrict a customer relationship should be risk-based rather than a means to avoid regulatory scrutiny. An institution should base the decision on the facts, circumstances and risk a relationship presents to the institution and then build a de-risking process that can be executed with consistency.
Conflicting Messages

Anti-money laundering (AML) de-risking is an emerging hot topic that continues to evolve. The guidance available to financial institutions today implies that it is alright to de-risk so long as a risk-based approach is taken. However, more recently the Financial Action Task Force (FATF) has turned its attention to the concept of de-risking to address some growing concerns that suggest financial institutions are going too far with their de-risking approach.

FATF defines de-risking as “the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than managing the risk (FATF, 2014).”

When one thinks about regulatory guidance that is available today and regulatory expectations that exist, one must ask, “Are their conflicting messages?” Unfortunately, U.S. regulators have not, and may never, define a clear process for institutions to follow in the management of the AML-related account closure decisions. Yet regulatory expectations exist and there continues to be turmoil over the subject.

Regulatory Guidance

Regulatory guidance on the subject of AML de-risking and case-by-case account terminations is minimal. Information that is available today is outdated and does not address current issues. In an older issue of The SAR Activity Review Trends, Tips & Issues publication there is one brief paragraph about “Cessation of Relationship/Closure of Account” (The Bank Secrecy Act Advisory Group, 2000):

“The closure of a customer account as the result of the identification of suspicious activity is a determination for an organization to make in light of the information available to the organization. A filing of a SAR, on its own, should not be the basis for terminating a customer relationship. Rather, a determination should be made with the knowledge of the facts and circumstances giving rise to the SAR filing, as well as other available information that could tend to impact on such a decision. It may be advisable to include the organization’s counsel, as well as other senior staff, in such determinations.”

When the USA PATRIOT Act was passed and enacted the following year on October 26, 2001, the issue of de-risking was addressed but for ensuring compliance with Section 326, Customer Identification Program (CIP). For example, The Federal Deposit Insurance Corporation (FDIC) statutes and regulations contain CIP requirements for banks to have written procedures that address situations when the bank should close an account after attempts to verify a customer’s identity (FDIC, 2014).

The Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA)/anti-money laundering (AML) Examination Manual was revised in 2010, and then again in 2014, but neither revision defined or expanded on the concept of de-risking. There remains a lack of guidance for institutions regarding how they should handle incidents when suspicious activity reports (SARs) are filed repeatedly on the same customer. Some institutions maintain a standard of three filed SARs before the relationship is terminated. The reality is that repeat SAR filings are often the central drivers for many institutions making case-by-case account closure decisions.
Surprisingly, Appendix S of the FFIEC BSA/AML Examination Manual does not depict account closures as a Key Suspicious Activity Monitoring Component (diagram shown below), yet within the Examination Procedures for Suspicious Activity Reporting, regulators are instructed to determine if “handling account closures” are included in the bank’s policies, procedures and processes for identifying, researching and reporting suspicious activity (FFIEC, 2014).

This diagram prompts more questions as to why there is a difference between the Appendix diagram and written exam procedures on the handling of account closures. Perhaps it was an oversight or did the authors of the FFIEC BSA/AML Exam Manual intentionally fail to address the practice of de-risking because of the complexity and controversy involved in exiting customer relationships? Regardless of the reason, account closures are indeed an extension of the suspicious activity monitoring process and they should be included in institutions’ AML investigations procedures. When institutions undergo audits or exams, the account closure process is of importance and is often in-scope for examination. A request for evidence of written procedures is made as part of an evaluation of the suspicious activity monitoring program.

The most regulatory guidance available on the subject of AML de-risk is from FATF. In October 2014, FATF issued preliminary guidance to provide banking supervisors and banks the key elements of taking a risk-based approach to mitigate identified ML/TF risk (FATF, 2014). The guidance was published with the intention of it being read in conjunction with the revised prior guidance on AML and TF measures and financial inclusion (FATF, 2013). The publication focuses on ensuring that AML and counterterrorism controls do not inhibit access to well-regulated financial services for financially excluded and underserved groups.
The Three E’s of De-Risking

Defining and implementing a well-documented account closure strategy requires knowledge of an institution’s risk appetite and time to build out closure steps necessary to manage the process effectively.

In my opinion, there are three key steps to carry out a case-by-case account closure strategy: (1) establish the institution’s risk appetite, (2) execute a consistent, repeatable and auditable process and (3) educate relationship managers on closure decisions.

Establish Risk Appetite

The first step in establishing an account closure strategy is to determine the institution’s risk appetite. Risk appetite is the amount of risk, on a broad level, that an organization is willing to take on in pursuit of value (KPMG, 2008). For example, some financial institutions may decide to not bank with certain customer types who may pose higher risks, such as MSBs, because of the increased cost of compliance responsibilities associated with ongoing know your customer (KYC), enhanced due diligence (EDD) and transaction monitoring activities. These decisions are often made at the senior management level and any decisions to exclude certain risky customer relationships should be addressed in the institution’s AML policy and referenced as necessary in line of business account opening procedures.

It is fair to assume that no reputable financial institution has a risk appetite for money launderers, therefore, criteria must be established to handle situations when the risk appetite levels for an institution have been exceeded. Effective AML compliance controls and regular AML risk assessments may prevent common pitfalls encountered by many banks and financial institutions. AML risk management compliance failures can have detrimental impacts on organizations of all sizes. In the case of a small credit union, North Dade Community Federal Credit Union, Shasky Calvery stated, “When a small institution opens its doors to the world, takes on greater risks than it can manage, and puts profits before AML controls, bad actors are bound to take advantage (FinCEN, 2014).”
Case Example

- In 2014 North Dade Community Federal Credit Union in Florida was assessed $300,000 in civil money penalties by FinCEN for AML failures related to management of high-risk international financial activity. The small credit union held $4 million in assets, with five employees.
- North Dade contracted with a third-party vendor and MSB to provide services and sub-accounts to 56 MSBs located in high-risk jurisdictions in Central America, the Middle East and Mexico.
- The outgoing wire transaction volume for 2013 alone was $1.01 billion in annual revenue by the MSBs. Total revenue generated for these accounts constituted 90 percent of the Credit Union’s annual revenue.
- FinCEN questioned, why would MSBs located all over the world choose a small Florida credit union?

Execute a Consistent, Repeatable and Auditable Process

After an institution has determined its risk appetite, the next step is formulating action steps to carry out account closure practices. There are several important factors to consider:

- Who should be notified of the closure decision?
- What types of risky accounts/relationships or customer behaviors warrant closure?
- When will recommendations for account closure occur?
- How do you prevent banned customers from returning to establish new account relationships?

There are many stakeholders to consider, such as the AML Investigative staff responsible for identifying closures, the BSA/AML officer, and the relationship manager(s). In some institutions, accounts are presented to an AML Oversight Committee, which may be comprised of various line of business compliance partners from across the organization. Some circumstances may require legal advice from the institution’s internal or external legal counsel.

Determining which risky accounts and relationships that will be referred for closure will vary by institution and will be based on the institution’s size, complexity and product mix. Consider a few common instances where a risky account or relationship may be referred for closure:

- Filling repeat SARs on the same customer for suspected BSA violations or ML
- Negative news that a customer has been indicted or convicted of ML
- A SAR filing for suspected TF
- Illegal Internet gambling activity
- High-risk international transaction activity that lacks transparency and legitimacy based on the due diligence performed and known customer facts
- An MSB, after attempts to educate, refuses to register with FinCEN and produce evidence of compliance with the BSA

Unless law enforcement has requested an account to remain open, some risky accounts or relationships may take a fast track to closure. An example would be a customer suspected of funding terrorism. Other risky relationships will be considered on a case-by-case basis and may be referred for closure after repeated unwanted behavior (e.g., after filing three or four SARs on the same customer).

Setting up controls for keeping unwanted or prohibited customers from entering or reentering the institution takes effort to manage effectively, but it is not infallible. Larger institutions build lists of customers who are prohibited from returning and automate controls to reject these customers at the onset of new relationships. Smaller institutions may conduct a manual search of their prohibited customers on a periodic basis. Whichever method is used, systems and processes change over time and established controls may need to be revisited and adjusted.

**Well-Documented Process**

Creating consistency and repeatability starts with developing well-documented written procedures that can be followed and understood by staff responsible for carrying out the process, as well as by auditors and examiners.

For institutions that do not have an AML Oversight Committee to present referrals to, the account closure key action steps may appear like this:

1. Using information obtained during the investigation (evaluation of KYC documents), AML investigations staff identifies account(s) or an entire relationship that meets the established criteria for termination.

2. The investigator completes a detailed Customer Relationship Exit/Account Closure Recommendation Form and compiles supporting documentation. Documentation must be provided to show a concise audit trail of information and dates that lay out the series of events such as initial detection, history of account monitoring and decision/reasons for recommended closure.

3. The completed Form is submitted to the designated individual(s), such as the AML investigations quality control coordinator and/or the AML investigations manager/director to determine if:
a. The referral meets the established risk-based closure criteria
b. The Form and corresponding supporting documentation are complete and defensible
c. There exists agreement between the AML investigations coordinator and managing director that the account(s) or relationship should be closed

4. Upon approval of the closure recommendation, the AML investigations manager/director will escalate the incident to the BSA/AML officer for approval to move forward with closure (by means of a regularly scheduled monthly meeting or more frequently depending on the type of referral case).

*Note:* Law enforcement may have an interest in keeping an account open, if so the request must be in writing. Ultimately the decision to close or keep an account open will rest with the financial institution.

5. If the BSA/AML officer approves, within five business days the closure referral is sent to the Loss Prevention or Account Operations staff. Loss Prevention or Account Operations is responsible for terminating the account(s) or relationship.

   a. The recommended account(s) or relationship is presented to the respective line of business relationship manager(s) for closure.
   b. **Agreement** - Stakeholders are in agreement and the account(s) or relationship is terminated within 30 to 60 calendar days. (Step 6)
   c. **Disagreement** - If stakeholders are not in agreement, the closure recommendation will be escalated by the AML investigations manager/director to the BSA/AML officer for a final decision.

6. The AML investigations staff follows up to ensure closure is completed within the agreed timeframe and places the customer(s) on the institutions “Prohibited Customer List” (PCL) or “Hot List.”

*Note:* Larger institutions may need to develop a tracking process to ensure accounts are closed within a reasonable timeframe.

Action steps should be clearly defined in the AML investigative procedures and should include actions that will be taken when disagreements occur or exceptions to policy occur. If exceptions to policy or procedures are encountered, a written detailed explanation of the
exception should be maintained. It should include a justifiable reason for the exception and include approval by the BSA/AML officer.

Auditability
Creating a lock tight closure practice is extremely difficult to accomplish seamlessly, but is important to ensure closure practices are carried out with consistency. When closure practices are independently tested by an institution’s internal or external audit service, expect examination of the following:

- Do written procedures exist? How well is the process documented through written procedures? Do the written procedures describe the entire process?

- If closed accounts are reviewed as part of the testing sample, are reasons that precipitated the closure documented?

- Is the closure process consistently executed the same way each time? In other words, is periodic quality control assessments performed to ensure detailed procedures are being followed as written?

- If an exception is identified, how was the incident resolved or the decision reached? For example, a customer’s account activity meets the set criteria for closure, but the line of business decides to accept the AML risk and the BSA/AML officer is in agreement with the decision. How are these situations managed? Do the written procedures cover these exceptions? If requested, can the AML staff produce evidence of documented exceptions?

- Has the BSA/AML officer or delegate formally approved the established closure process? Can the AML staff provide evidence of the approval?

- Has the AML staff built metrics to keep senior management well-informed of the number of account closures that have occurred on a monthly or periodic basis?

In addition to the expectation of written procedures, audit will evaluate risk assessments to determine if AML staff understands the institutions’ risk (i.e., customer, products/services and geographic risk). Audit will generally take an interest in high-risk businesses and customer types that are classified as high risk. There will be an expectation that appropriate controls have been implemented to manage the risk. For example, if certain customers (e.g., non-resident aliens) are inherently high risk, controls should reflect that customers are risk rated accordingly and are monitored more frequently. Expect audit staff to select a targeted sample that includes higher risk customers types such as MSBs, politically exposed persons (PEPs) or customers risk rated as high.

An audit plan and scoping is generally contingent on how the organization operates. If there are certain lines of business that are inherently high risk or controls are knowingly
weak or lacking, the audit plan will be built accordingly to address these areas. In such cases, at a minimum, an annual audit should be expected.

**Educate Relationship Managers**

When the account closure criteria and written process have been developed and implemented, it is important to educate the relationship managers on the closure process. A high-level overview of criteria that may warrant account termination should be provided. The key is to keep the training concise and ensure employees understand the importance of such risk decisions and the institutions’ AML compliance culture.

It is essential to cover the confidential nature of such decisions. As with most cases, a SAR may have been filed and it is crucial that the employee take care not to ‘tip off’ a customer who is upset at the company’s decision to close their account. Relationship managers should be reminded that a bank has the right to exit a relationship for any reason. This right is usually covered in the Account Agreement or the Bank Services Agreement provided to customers when they open an account. Relationship managers should be trained to be discreet and reference the agreement disclosure in these cases. Some institutions may decide to develop scripts for communicating these decisions with customers when needed. A script is usually helpful for Call Center staff who may speak with a customer over the phone and who have limited knowledge about the account relationship.

If an institution has decided to form an Account Closing Committee or an AML Oversight Committee, training can be conducted with the respective line of business Committee Members. The Committee Member can be responsible for disseminating the training to additional line of business stakeholders/relationship managers.

**Law Enforcement Requests**

Law enforcement agencies may occasionally have an interest in ensuring a particular account remains open. If a request is made to keep a particular account open, financial institutions are instructed by FinCEN to ask for the request in writing (FinCEN, 2007). The written request should indicate that the agency has requested the financial institution maintain the account, the purpose of the request and duration (not to exceed six months). After six months a subsequent request may be made by law enforcement to keep the account open for a longer period of time.

Ultimately, financial institutions have the right to maintain or close a customer account. If a decision is made to fulfill law enforcement’s request, the financial institution must adhere to all aspects of the BSA record keeping and reporting requirements, such as requirements to file SARs, even when keeping an account open for law enforcement. Reference the “Resources” section for a Sample Keep Open Letter.
Managing Disagreements

Often there are disagreements between AML compliance staff and business stakeholders with decisions to close an account or restrict a relationship. These instances should be managed carefully and with diplomacy. Building relationship trust and strong compliance partnerships can be difficult but they are essential to keeping open dialog and it goes a long way towards building stakeholder buy-in.

Influencing management that exiting a customer account or relationship is the best risk-based decision can be tricky. AML staff may be passionate about exiting a customer relationship and they may have good cause. Ultimately the BSA/AML officer should have the authority and support of the board to make final decisions when a customer relationship needs to be discontinued. In order to reduce the number of disagreements, the AML staff must be prepared with all of the documented facts and circumstances needed to easily convince senior management that account closure is the best course of action. It is hard to argue with the facts. If the BSA/AML officer is pulled into discussions and he or she has to explain the reason for the closure, he or she should be fully briefed and knowledgeable of the closure case and reasons that triggered the decision.

There are times when the line of business relationship manager will disagree with the decision. If the relationship manager has worked hard to establish a total financial services relationship (also called product bundling), he or she may be biased toward keeping the relationship. They may argue that the relationship is harder to unwind or that the customer is profitable. To reiterate, preparation is essential.

It may be worth explaining what goes into AML monitoring and customer due diligence (CDD) processes, the number of AML staff dedicated to these functions and calculating the estimated total number of hours spent on monitoring, documenting and building the closure case for a particular customer. In the end, these functions reduce total customer profitability. There are plenty of case examples that can be used as references to demonstrate the potential financial and reputational damage that can occur if risky customer relationships are mismanaged.

BSA/AML Penalty Cases

Below are a few examples summarized on BankersOnline.com in which financial institutions were assessed monetary penalties or Cease and Desist Orders (C&D) for BSA failures related to risk assessments and mismanagement of high-risk customers (BankersOnline.com):

- **Oppenheimer & Co, Inc.** – In 2015, FinCEN and the Security Exchange Commission (SEC) assessed $20 million in civil money penalties (CMP) for willfully violating the BSA. The securities broker designated a customer which was a foreign financial institution as high risk, but failed to assess the institution’s specific risk, inadequately monitored transactions and did not detect or investigate numerous suspicious transactions conducted through the account (illegal penny stock trading).

- **Eastern National Bank** – In 2008, the OCC issued a C&D to the federally-charted bank located in Miami, FL, for various BSA violations. As part of the agreement,
board of directors were directed to develop, implement and ensure bank adherence to policy. The bank was instructed to establish a policy that defines when the bank:

- Will not open, block use of or close an account (and file appropriate SARs)
- Determines that continuing the relationship would be detrimental to the bank’s reputation

**Dover N.J. Spanish American Credit Union** – In 2007, the National Credit Union Administration (NCUA) issued a C&D order because the credit union lacked an adequate formal BSA/AML compliance program. The credit union was directed to:

- Identify all members who were MSBs
- Establish an effective MSB monitoring program within 30 days
- Close all MSB accounts for which due diligence could not be completed within the set timeframe

**Enduring Challenges**

There are many competing forces at work when communicating an account closure decision, such as employee incentives for opening new accounts, the backend compliance costs and potential financial/reputational risk exposure. The type of customer may also present a challenge, such as a customer who is a friend, business partner or relative of a board member.

**Connecting Relationship Dots**

Depending on a financial institution’s size and complexity, there may be situations when it is difficult to connect the relationship dots. Determining how many accounts a customer has and if there are related customers involved in the suspicious or risky unwanted behavior may present a challenge. Larger institutions commonly encounter difficulties because there are numerous customer account record systems rather than a central repository that comprises the entire customer relationship. If an entire relationship is being terminated, it may be challenging to determine the extent of the relationship and, unknowingly, a partial relationship will remain unchecked and the risk exposed.

**Relationships that are Impossible to Terminate**

Some accounts are impossible or extremely difficult to terminate, such as customers with credit lines or lending relationships. It is simple to stop a customer from gaining access to additional funds on a credit line, but steps must be taken to provide a reason for the stop. What if a customer has maxed out their credit limit? Most lenders want to ensure repayment of funds rather than tipping off the customer of its intent to terminate the relationship and create a charge off situation. The same difficulty exists for other various lending relationships such as mortgage loans, automobile loans or large business loans.

Sometimes financial institutions have to ‘care for’ the lending relationship rather than exit the relationship. This may mean adding the customer’s name to institutions lists of customers who are prohibited from establishing additional lending relationships.
There is a debate among banking professionals as to whether the Consumer Financial Protection Bureau (CFPB) will eventually creep over to address Safety and Soundness regulations, specifically the treatment of consumers as part of a bank’s AML account closure practices. The Dodd-Frank Act granted rule-making authority to the CFPB to supervise enforcement compliance of the Equal Credit Opportunity Act (ECOA), Regulation B (CFPB Consumer Laws and Regulations, ECOA, 2013). ECOA applies to all creditors who are responsible for informing credit applicants of the specific reasons for account denial. If AML reasons are in play, creditors must take care not to violate specific requirements when a Notice of Adverse Action reason is given to a credit applicant. AML compliance staff should seek legal advice when crafting a specific reason for credit denial based on an AML reason.

**Continued Surveillance (Prohibited Customer List)**

Closing a high-risk account does not alleviate a financial institution’s compliance burden. Rather, continued surveillance must prevail if unwanted customers are to be kept from reentering and reestablishing new relationships. Continued surveillance is generally performed by placing customers on a Prohibited Customer List (PCL). Some other common names are “Hot List” or “Black List” where automated or manual screening occurs daily or periodically to identify any attempts to open new accounts. If unwanted customers are successful, AML compliance teams have to address these events quickly.

For larger institutions, several PCLs will be necessary because of various customer data repositories/system applications used to open new accounts. This increases the complexity of institutions’ surveillance responses and the potential for a systematic breakdown.

To decrease the possibility of surveillance failures, partnerships should be entered into with information technology (IT) teams in order to build periodic data validation tests to prevent or catch data feed failures or data quality issues. The culprit is often tied to systems that are replaced over time or systems upgrades that cause data feed incompatibility. Formal data validation processes should be established and should include steps to properly escalate and prioritize the responses to any gaps identified in order to ensure timely remediation.
Final Comments

Unintended Consequences

De-risking is subjective and therefore, each financial institution will approach de-risking differently. The common drivers of de-risking are generally based on concerns with customer profitability, regulatory compliance administration efforts/costs and the potential financial/reputational harm that can occur when risky customer relationships are not properly managed. As a result, many financial institutions make hard decisions on what their risk appetites will be. As a result, certain risky business relationships and customers are terminated or restricted.

There are two critical reasons FATF has committed to addressing issues with de-risking (FATF, 2014):

1. De-risking can introduce risk and opacity into the global financial system, as the termination of account relationships has the potential to force entities and persons into less regulated or unregulated channels. Moving funds through regulated, traceable channels facilitates the implementation of anti-money laundering/counter-terrorist financing (AML/CTT) measures.

2. It is central to FATF’s mandate to ensure that the global AML/CTF standard is well understood and accurately implemented, and the countries and their financial institutions are provided with support in designing AML/CTF measures to meet the goal of financial inclusion.

FATF Recommendations require financial institutions to terminate customer relationships, on a case-by-case basis, where the ML/TF risks cannot be mitigated. This recommendation goes hand-in-hand with the risk-based approach message FinCEN has recently provided to financial institutions, as well as the existing U.S. regulatory guidance that suggests an account termination decision should be made on the facts and circumstances rather than the filing of a single SAR.

Without question, the subject of AML de-risking will linger as a hot topic for some time as compliance costs magnify and regulatory pressure continues to build. The key will be forthcoming improved and consistent regulatory guidance that helps financial institutions develop and implement risk-based plans to effectively manage high-risk relationships, while also providing much needed financial transparency.
WORKS CITED


Resources

- **FinCEN Statement on Providing Banking Services to Money Services Businesses** – This statement reiterates FinCEN’s expectations regarding providing banking services to MSBs. FinCEN believes institutions can serve the MSB industry while meeting requirements under the BSA.

- Requests from Law Enforcement - Sample Keep Open Letter

![Sample Keep Open Letter.pdf]