Detecting Hidden Risks:
An Investigative Approach to AML Audit in Community Banks

By: Dan Jackson, CAMS, CPA, CRCM
Table of Contents

I. Introduction
   a. The objective of the Bank Secrecy Act
   b. The Community Bank defined

II. Implications of Hidden Risks in AML Programs
   a. Worst Case Scenarios
      i. Penalties
      ii. Enforcement Actions

III. Potential Hidden Risks within the Community Banks AML Program
   a. The Customer Identification Program (CIP) and Customer Due Diligence (CDD) Program
   b. Money Services Businesses (MSBs)
   c. Wire Transfers
   d. OFAC
   e. PEPs

IV. Conclusion

V. References
I. Introduction

The intention of this paper is to provide consideration and discussion on the impact of hidden risks within the Anti-Money Laundering (AML)/Bank Secrecy Act (BSA), including the Office of Foreign Assets Control (OFAC), programs of community banks. The collective efforts will hereafter be referred to as the AML program. This paper will explore potential areas in which components of the AML program may be overlooked and expose the institution to unwanted risk. In identifying these potential areas of risk, it is possible to identify processes and procedures to enhance controls over these areas to mitigate those risks. In order to correctly consider these implications, the focus should be on the ultimate goal or objective of the program. While products and services offerings have changed over the years with the introduction of technology and the significant advances of that technology, let us consider the intent of the Bank Secrecy Act.

“The Currency and Foreign Transactions Reporting Act of 1970 (which legislative framework is commonly referred to as the "Bank Secrecy Act" or "BSA") requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering.” (1)

The basic tools to detect and prevent predicate crimes, from terrorist financing to human trafficking, begins with the institution’s risk assessment. The risk rating process will begin, but not necessarily end, with the documentation of risk with respect to products, services, customer base, and location among other factors. The internal control element, being one of the current four cornerstone pillars of a BSA program, will be carried out through the establishment of an institution’s policies and procedures. The remaining pillars – designation of a BSA officer, a comprehensive training program, and an independent audit – will form the basis for carrying out this program with institutions addressing these elements to varying degrees. Only after a review of these elements may a determination on the sufficiency of the institution’s program be made. The primary objective of meeting regulatory expectations or independent audit requirements has been achieved but satisfaction that the program provides the level of desired comfort may be a different story. Ultimately, the Board of Directors must identify their “risk appetite” with respect to the sufficiency of its AML program and whether the current policies, procedures, and audit function meet the objectives based on the acceptable level of risk.

Regulatory scrutiny will be at its highest when significant program deficiencies are identified. However, the potential exists, in spite of previous successful regulatory examinations and independent audits that a single, unidentified risk could result in potentially significant consequences. The resultant issue could, in fact, be partially due to prior examination and audit successes. This one-time, isolated incident could be the failure to identify a known money launderer or terrorist financier or simply the failure to properly search and act upon the existence of an individual or organization that is identified as a Specially Designated National or SDN. This introduces the element of reputational risk. Whether it be a financial institution in a small
community or a larger city, this risk is difficult to repair when it relates to highly sensitive, publicly communicated BSA failures or deficiencies.

Over the years, many institutions, while not having perfected them, have become efficient at addressing the BSA Federal Financial Institutions Examination Council (FFIEC) core examination procedures. In some cases, this has likely resulted in the over-reliance on the current line of thinking, which resulted in operating on cruise control with respect to the upkeep of policies and procedures. This is an easy trap to fall into as the institution has exited several regulatory examinations and independent audits with no findings of consequence. The view of the AML program is that the control environment is strong, management takes pride in their ability to monitor processes and procedures, and the institution’s history reflects these beliefs. Known products and services, a known customer base, and understanding of the institution’s program are all potential factors as to why there may be a failure to identify future risks and over-rely on the status quo.

**What institutions are being discussed?**

The community bank can be defined in part on asset size but location and products and services play a part as well; however, there is no universal definition. The following serve as references for assisting in defining the community bank. The FDIC disclosed during the Summary of its *Defining the Community Bank* that, “Community banks mainly conduct lending and deposit gathering activities within a fairly limited market area. They are said to be relationship lenders, which rely to a significant degree on specialized knowledge gained through long-term business relationships. They are likely to be owned privately or have public shares that are not widely traded, and therefore tend to place the long-term interest of their local communities high relative to the demands of the capital markets.”

Historically, the community bank was defined based on asset size with a standard definition of $1 billion in assets.

The Office of the Comptroller of the Currency further supports this threshold and states the following, “Community banks are generally defined as banks with less than $1 billion in total assets and may include limited-purpose chartered institutions, such as trust banks and community development banks.”

For purposes of this paper, the traditional asset threshold of $1 billion as a general guideline will be used; however, many of the concepts and considerations discussed herein would apply to institutions of many sizes based on the fact that they have a fairly limited marketing area, have a limited offering of products and services, and a predominant concern is serving their customers. Per the “FDIC Quarterly Banking Profile” First Quarter 2016 submission, community banks represent 93 percent of financial institutions and account for 44 percent of small loans to businesses. The total number of reporting insured institutions for this period was 6,122.
II. Implications of Hidden Risks in AML Programs

As an institution moves forward with its AML program, it must not become complacent. Many aspects of banking require a proactive approach in order to maintain safety and soundness within an organization. That is no different for the AML program. There are several factors that may lead to complacency, or perhaps overconfidence in the program. Other identified risks within the institution may require more immediate attention. Strong leadership will elevate those greater risks to the forefront and dedicate time and resources based on the perceived risk. Institutions have a number of risk assessments, but they are not the same across all institutions. Generally, an institution will have an Information Technology risk assessment and an AML risk assessment. A number of institutions will have an enterprise-wide risk assessment. There may be varying degrees of audit risk assessments within institutions while some do not have formally, documented risk assessments for their audit areas. For virtually any risk assessment, there is a significant amount of subjectivity and within the community bank environment significant variations in the documentation with respect to these audit risk assessments will be found. With all risk assessments that tie into the audit function, the degree of risk is relative, which again can be subject to interpretation. Management will state they know where their risk lies. That belief may be true, but the potential exists for unidentified, elevated risk factors. Within the community bank environment, these factors may be the result of long standing customer relationships, long tenured personnel, often with strong interpersonal customer relationships, and self-designed internal controls. As a result, complacency within the community bank may ultimately result in the failure to identify additional risks.

Within the FFIEC BSA manual, it states, “….risk assessment has been given its own section to emphasize its importance in the examination process and in the bank’s design of effective risk-based controls.” Considerable time and effort are spent in identifying risks and implementing controls to mitigate those risks. These processes are necessary in order to achieve a satisfactory rating or audit outcome. These satisfactory ratings may result in overconfidence that all sources of risk to institution have been identified, thus, allocating resources elsewhere and losing the proactive mentality often necessary to identify risks.

The potential failings in relation to this risk may be due to poorly designed controls, which may be in part due to the failure to identify risks. As new products or services are introduced into the marketplace not all risks are readily identifiable. As the product or service progresses and grows, additional risks become known and can be incorporated into the risk assessment, which then flows into the audit plan. Often, mistakes must be made in order to learn from those mistakes and improve the process. The community bank may become overconfident in its ability to mitigate its risk or simply be complacent due to previous success in examinations and audits. The potential ramifications of failing to identify, failing to react, or failing to monitor existing and/or new products and procedures must be considered and evaluated.
In any regulatory examination or independent BSA audit, a single or isolated exception or violation will not typically result in a significant finding, but that depends on the severity or ultimate result from that individual issue. Often, program deficiencies are identified due to significant failings over a period of time rather than a single point in time. With that being said, the original objective of the AML program was to detect and prevent money laundering. Potentially, a single failing within the AML program could result in the failure to detect or prevent money laundering. That single incident could result in significant negative consequences such as enabling a financial crime resulting in a terrorist plot. In such a case, public perception may result in a negative pushback before a regulatory agency has the opportunity to finalize its findings.

With program deficiencies, repeated over a period of time, the institution may subject itself to regulatory actions including the assessment of fines and penalties. As identified in public enforcement actions, severe actions against institutions are the result of widespread deficiencies in the institution’s program that are pervasive over a period of time.

**What do the trends say?**

FinCEN produced the SAR Stats Technical Bulletin in October 2015, which presents the annual review of aggregated Suspicious Activity Report (SAR) filing activity. This information, while still being presented annually, will be available interactively on the website. The publication reflects a substantial increase in Suspicious Activity Report (SAR) filings from 2012 to 2014.

**Exhibit 1: Filings by Year & Month by Money Services Business (MSB)**

<table>
<thead>
<tr>
<th>Month</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>-</td>
<td>14,919</td>
<td>57,353</td>
</tr>
<tr>
<td>February</td>
<td>-</td>
<td>10,203</td>
<td>55,217</td>
</tr>
<tr>
<td>March</td>
<td>7</td>
<td>19,746</td>
<td>55,700</td>
</tr>
<tr>
<td>April</td>
<td>327</td>
<td>37,366</td>
<td>64,642</td>
</tr>
<tr>
<td>May</td>
<td>632</td>
<td>58,562</td>
<td>57,753</td>
</tr>
<tr>
<td>June</td>
<td>1,083</td>
<td>44,577</td>
<td>63,961</td>
</tr>
<tr>
<td>July</td>
<td>4,102</td>
<td>43,846</td>
<td>57,667</td>
</tr>
<tr>
<td>August</td>
<td>5,195</td>
<td>45,074</td>
<td>54,290</td>
</tr>
<tr>
<td>September</td>
<td>6,037</td>
<td>45,729</td>
<td>64,317</td>
</tr>
<tr>
<td>October</td>
<td>6,308</td>
<td>59,559</td>
<td>62,385</td>
</tr>
<tr>
<td>November</td>
<td>15,116</td>
<td>48,535</td>
<td>66,810</td>
</tr>
<tr>
<td>December</td>
<td>12,075</td>
<td>62,899</td>
<td>60,890</td>
</tr>
<tr>
<td>Subtotal</td>
<td>50,882</td>
<td>491,015</td>
<td>720,985</td>
</tr>
<tr>
<td>Total Filings</td>
<td></td>
<td>1,262,882</td>
<td></td>
</tr>
</tbody>
</table>
From 2012 to 2014, SAR filings by MSBs increased by over 1,300 percent.\(^6\) This trend over the two year period should highlight a risk within financial institutions that is not necessarily emerging but is more quantifiable. With MSBs filing an increasing number of SARs, the risk of any financial institution doing business with an MSB increases. As these entities file more SARs, they are self-identifying themselves as at higher risk of money laundering or terrorist financing. The risks of unidentified MSBs will be explored in the next section.

**Exhibit 1: Filings by Year & Month by Depository Institutions**  
March 1, 2012 through December 31, 2014

The statistics include Suspicious Activity Reports filed since March 1, 2012 on FinCEN Form 111 where the type of financial institution is depository institutions (i.e., banks, thrifts, savings and loans, and credit unions).

<table>
<thead>
<tr>
<th>Month</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>-</td>
<td>12,232</td>
<td>72,201</td>
</tr>
<tr>
<td>February</td>
<td>-</td>
<td>21,088</td>
<td>67,184</td>
</tr>
<tr>
<td>March</td>
<td>24</td>
<td>45,719</td>
<td>70,226</td>
</tr>
<tr>
<td>April</td>
<td>609</td>
<td>67,278</td>
<td>78,925</td>
</tr>
<tr>
<td>May</td>
<td>1,210</td>
<td>72,255</td>
<td>80,569</td>
</tr>
<tr>
<td>June</td>
<td>1,713</td>
<td>63,579</td>
<td>74,499</td>
</tr>
<tr>
<td>July</td>
<td>2,505</td>
<td>70,857</td>
<td>78,528</td>
</tr>
<tr>
<td>August</td>
<td>3,115</td>
<td>74,312</td>
<td>73,576</td>
</tr>
<tr>
<td>September</td>
<td>2,947</td>
<td>68,751</td>
<td>73,444</td>
</tr>
<tr>
<td>October</td>
<td>5,561</td>
<td>79,201</td>
<td>80,490</td>
</tr>
<tr>
<td>November</td>
<td>7,954</td>
<td>69,631</td>
<td>66,123</td>
</tr>
<tr>
<td>December</td>
<td>10,098</td>
<td>69,027</td>
<td>71,162</td>
</tr>
<tr>
<td>Subtotal</td>
<td>35,736</td>
<td>713,930</td>
<td>886,927</td>
</tr>
<tr>
<td>Total Filings</td>
<td>1,636,593</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As with the MSBs, the trend is increasing for SAR filings at depository institutions but at a greater rate than MSBs – 2,382 percent since 2012. As each year passes, more institutions are taking advantage of the AML programs to assist in the identification of suspicious activity. With the advent of the E-filing system in 2013 and the increased proliferation of electronic monitoring, it is understandable that the volume of SAR filings would increase. The introduction of the electronic filing shows a significant increase in SAR filings in 2014 over 2013 for both depository institutions and MSBs.

In today’s regulatory environment, regulatory requirements and expectations are shifting at a fast pace and require a consistent, team oriented approach for the betterment of the program. What
was acceptable last year may not be acceptable next year. What is acceptable from a procedural standpoint yesterday may not be acceptable tomorrow. This environment is resulting in larger institutions de-risking and no longer banking many MSBs. With these entities in need of financial services, they will seek to find these services at smaller institutions such as the community bank.

The reporting of suspicious activity is trending upward. The ramifications that relate to this trend will be explored with the discussion of enforcement actions.

**Enforcement Actions Hitting Home**

Money Services Businesses have been subjected to enforcement actions/fines from FinCEN. During the period from January 2015 through April 2016, five MSBs were assessed civil money penalties. Per the Audit Report from the Office of Inspector General, OIG-16-006, \*BANK SECRECY ACT, FinCen Continues to Face Challenges with Money Service Businesses, “We did note that in 2012 and 2013, FinCEN did not have a single enforcement action against an MSB but between 2014 through June 2015, FinCEN had nine such cases.” (7) This highlights the importance of identifying and monitoring MSB customers.

For the period beginning January 2015 through April 2016, three depository institutions have been assessed enforcement actions/fines from FinCEN. Examples of those include the following:

FDIC supervised institutions of note:

- The Bank of Mingo of Williamson, West Virginia was assessed a $4.5 million civil money penalty for willfully violating the Bank Secrecy Act. The bank admitted to violation of the BSA. Of note with respect to this discussion is the institution size and location. The bank maintained six locations within Mingo County, West Virginia, with a population of less than 30,000. The bank’s asset size was less than $100 million. All factors indicate that the institution indeed meets the definition of a community bank. The order states, “Mingo had systemic BSA violations that derived from its failure to establish and maintain an adequate anti-money laundering program and customer due diligence program. Mingo’s program deficiencies led to its failure to monitor, detect and report suspicious activity and to timely file currency transaction reports. Consequently, from 2008 through 2012, Mingo allowed more than $9.2 million in structured and otherwise suspicious cash transactions to flow through the institution unreported.” (8) The amount of the penalty assessment was $3.5 million, assessed by the FDIC as primary regulator. Among the primary issues identified were the failure to implement an appropriate Customer Identification Program and the failure to report suspicious activity, in part due to failings in its high-risk account identification and monitoring. FinCEN assessed a penalty in addition to that of the FDIC.

- Meetinghouse Bank, of Boston, Massachusetts was issued a Consent Order in April 2016. The items the bank must do in response to the Order include, but are not limited to, the
completion, including documentation, of a BSA risk assessment and the establishment of “appropriate” written policies and procedures. The FDIC deemed the pillars of a BSA program as inadequate ultimately resulting in the Order. The bank has $123 million in assets. (9)

And those identified with the OCC as the primary regulator:

- A Consent Order was issued to Stearns Bank, N.A., St. Cloud, Minnesota, in April 2016. The Order stipulates that the bank failed to adhere to its internal policies and procedures with respect to suspicious activity. The bank also failed to timely file Suspicious Activity Reports (SARs). Civil Money Penalty - $1,000,000. The bank has $1.9 billion in assets. (10)

- Gibraltar Private Bank and Trust Company, Coral Gables, Florida. The bank was assessed a civil money penalty in the amount of $2,500,000 in February 2016. The Federal savings association was under a consent order from 2010 and subsequent examinations identified the failure to file timely SARs resulting in what was considered deficiencies in the bank’s BSA/AML program. The bank has $1.6 billion in assets. (11)

- First National Community Bank, Dunmore, Pennsylvania, consents to a $500,000 civil money penalty in February 2015 for the failure to file SARs on a timely basis covering a period of five years. A significant issue with respect to the filings involved a board member, Michael Conahan, who was subsequently sentenced to prison and ordered to pay restitution. A subpoena was delivered to the bank regarding this director; however, the appropriate red flag was not identified resulting in additional review. FinCEN assessed an additional $1 million penalty concurrently with the OCC imposition. (12)

The Federal Reserve takes action:

- Commerce West Bank, Irvine, California, with assets of $473 million on April 12, 2016 is required to submit a BSA/AML compliance program that includes customer due diligence, suspicious activity monitoring and reporting, and currency transaction reporting among other requirements. Part of the requirement is to conduct a review of high-risk accounts to determine suspicious activity. (13)

- National Bank of Pakistan, through a branch office in New York enters into a written agreement with the Federal Reserve Bank of New York and the New York State Department of Financial Services as of March 14, 2016. Among the requirements for compliance include plans to address the Office of Foreign Assets Control (OFAC), the customer identification program and suspicious activity monitoring and reporting processes. With respect to OFAC compliance, the Bank and branch are called on to improve the screening process, document review and disposition, enhancing procedures, and update its risk rating process. (14)
Industrial Bank of Korea, Seoul, Korea, through a branch office in New York enters into a written agreement with the Federal Reserve Bank of New York and the New York State Department of Financial Services as of February 24, 2016. The BSA program, including suspicious activity reporting, enhancements are requirements of the agreement. The bank and branch shall jointly submit a written plan for compliance with OFAC regulations, which shall include the following, “(a) policies, procedures, and periodic testing to ensure that the OFAC designated parties list is current and includes all OFAC specified countries, entities, and individuals; and (b) procedures to ensure that the processes used to suppress repetitive false positives are periodically reviewed and updated to ensure appropriateness and relevance.” (15)

With respect to the community bank, fines and penalties have never been more prevalent for AML related deficiencies than in today’s community banking environment. As reflected in the above examples, institutions of various sizes in various locales under the guidance of a regulatory agency is subject to federal regulation and the failure to comply or introduce undue or unmonitored risk subject any community bank to similar consequences. Within the community banking environment, the risk of maintaining relationships with MSBs and non-bank financial institutions increases as those customers file increasing numbers of suspicious activity reports. The proper identification of risks and the implementation of adequate controls and monitoring processes are of the utmost importance. With the potential of MSBs seeking new banking relationships at the community bank level in addition to the longer tenured MSBs already banking at these community banks, these risks will be elevated.

### III. Potential Hidden Risks within the Community Banks AML Program

The objective of this paper is to identify hidden risk areas within the community bank environment. There are several methods by which trends can be identified within the AML community. One of the primary methods for this communication is the regulatory enforcement actions as identified above. Regulatory guidance and informative publications also provide relevant information. With respect to enforcement actions, it is quite clear that a severely lacking program will result in negative consequences. In the OCC’s Semiannual Risk Perspective, Spring 2016, it warns that banks’ decisions to terminate customer relationships due to the risk they present may shift that risk to others who may not be prepared to identify or properly manage the necessary monitoring for these entities. (16) As noted previously in the FDIC’s quarterly report, the community banks represent 44 percent of small loans to businesses in the United States. With the pressure to identify and book loans in today’s environment, institutions may be willing to accept additional risk in an area that represents good potential for growth. Additionally, the report warns that banks may have shortcomings in the development of adequate controls as products and services change based on increases in technology.
The ultimate objective of an AML program is to identify suspicious activity and to properly report that activity in the manner and within the timeframes established within the Act. Financial institutions inherently have risks to AML compliance, but the community bank will have some hidden risks due to their known customer base, limited product and service offerings, and history of satisfactory compliance. Being a “small community bank” with no significant AML deficiencies in the past increases the potential for hidden risks within the institution. In order to identify suspicious activity, a strong understanding of each customer must be obtained – who they are, what it is that they do, and how they intend to use bank services. There are several ways this information can be obtained, which includes a strong due diligence program at account opening that is formally and thoroughly documented, a review of account history including the types, number and amounts of transactions, identification of all requested products and services, and even a visit to their place of business, if deemed appropriate. In order to properly obtain this information, a strong training environment is necessary. Once these processes are in place, future activities will often fall into a back office review. Certainly, front-line personnel are required to be aware and educated on what may be suspicious. A teller should be able to identify structuring and any potential evasion for the reporting requirements. It is not a stretch to assume that an accomplished money launderer or terrorist financier would be able to structure their business to pass through the front-line with little problem.

Monitoring is key, but the how, when, and what to review may prove difficult. The how is in part determined on whether the institution has AML software to assist in the monitoring. If software is not in use at the institution, the task of identifying activity to review becomes more difficult although likely less time consuming. The when of monitoring is easily answered from the perspective of when the monitoring must be documented based on current policies and procedures, but the question may arise as to whether the frequency is adequate given the customer base. The what is likely more difficult for those without software as decisions must be made as to the degree of research or review for identified accounts. Community banking management will have to provide the answers to the questions based on the allocation of time with respect to the identified risk.

To this point, the case has been built that suspicious activity must be identified and reported. From a program perspective, processes, procedures, products, and services should be periodically reviewed to identify potential areas for which an institution may not properly identify the customer and the appropriate usage for their account.

**The Customer Identification Program (CIP) and Customer Due Diligence (CDD) Processes**

The failure to properly assess the risk associated with new customers and fully document the use of the account weakens the institution’s AML program. The FFIEC BSA manual core procedures call for a sampling of new accounts to include accounts without taxpayer identification or other incomplete but required information, accounts identified as higher risk, or those opened by a third
party. The documentation with respect to risk ratings varies from one institution to another. An institution may have a self-created scoring system, a judgmental system, not based on quantifiable procedures, or a limited system that does not formally rate its customers. The documentation supporting that designation also will vary from institution to institution. It is highly recommended that an institution reassess its risk rating process at account opening and document its final decision. The risk rating and identification process may be determined that only business accounts incur the additional due diligence, for example, deemed to ultimately present the greatest risk to suspicious activity.

Historically, the required elements under CIP – name, physical address, date of birth, and taxpayer identification – have been obtained and retained on file. The variation in which community banks document the customer relationship beyond these factors limits some institutions in their ability to monitor these accounts in the future. In many cases, institutions with limited rating processes will automatically rate a significant majority of these new customers as “low” risk. Additionally, an institution will have many legacy customers that will not undergo the formal CIP requirements and CDD documentation process as they were established prior to implementation of the CIP requirement in 2003. The failure to adequately establish and review these “low” risk customer’s accounts could pose undue risk to the institution and could allow these customers to engage in undetected, unlawful activity. Longevity and familiarity can lead to complacency in critically reviewing account activity and maintaining a skeptical view as it relates to account monitoring and subsequent risk ratings. The failure to properly risk rate the institution’s customers would lead to less frequent monitoring and likely the failure to properly report suspicious activity. As a result, the account opening process and documentation, as well as the periodic review of the institution’s risk rating process, should be critically reviewed. A number of community banks rely on a manual process and have limited resources for account monitoring that lends itself to the potential of failing to identify suspicious activity resulting in under-reporting or the failure to file timely SUSPICIOUS ACTIVITY REPORTS.

**Money Services Businesses (MSB)**

The primary concern is the risk of failure to identify an MSB or other high-risk customer type. If shortcomings are found in due diligence programs under CIP, the shortcoming may result in the failure to identify an MSB resulting in an incorrect initial risk rating. A robust and well-documented customer due diligence and enhanced due diligence program may be in place. The account usage and the types of transactions and volume levels may be documented.

One reason these accounts may not be identified as an MSB could be that the customer did not represent themselves as one and subsequent reviews showed that the anticipated activity, as documented at account opening, was achieved. The entity may actually be registered as an MSB but failed to properly communicate that fact.
For future consideration with regards to beneficial ownership, the following is a useful reference point from the Office of Inspector General Audit Report, OIG-16-006, “MSBs must re-register with FinCEN no later than 180 days after it has a change in ownership requiring it to re-register with the state, a transfer of more than 10% voting power or equity interests, or more than a 50% increase in agents during the registration period.” (17)

For further emphasis on the beneficial ownership Customer Due Diligence (CDD) rule, the beneficial owners must be identified at account inception. These owners would include those with 25 percent ownership. Additionally, the party charged with controlling, managing, or directing the entity also would need to be identified under the beneficial rules. The elements required under CIP — name, physical address, date of birth, and taxpayer identification number — would be required of beneficial owners. The rule affects new accounts opened on or after May 11, 2018. The impact on community banks will be limited for many of its accounts; however, larger commercial relationships may present a greater risk. For example, in a number of smaller institutions there may be requests for commercial real estate loans, for which all the principals do not have an existing relationship, are out-of-area or do not represent the traditional “relationship” banking customer. For an institution wishing to make high quality loans, these types of loans may be too difficult to pass up.

From an audit perspective, the MSB listing can be generated from the FinCEN website and compared to the database or a particular customer. The parameters may be imperfect, but the test provides additional comfort that any potential MSB customers have been identified. The impact of this search and identification of MSBs will assist us in that a customer that should be identified as a high risk, resulting in more frequent monitoring, is categorized as such. It also identifies a customer who may not have been as forthcoming as desired, which may elevate the risk rating to a higher category.

As previously discussed, FinCEN is providing Money Services Businesses with an increasing amount of attention. The businesses themselves are now reporting more suspicious activity. This increases the risk to any institution that acts as their depository institution. As with the CIP program, the BSA examination manual provides guidance on review and documentation standards for MSBs. From an audit perspective, these factors should be tested – the registration and renewal process, the monitoring of the money services business activities, the consideration of the customer’s policies and procedures with respect to the BSA. For those readily identifiable as MSBs, a well-defined process and subsequent monitoring is more easily implemented.

With regards to activity monitoring, an unregistered MSB may be identified, for example, as the customer cashes checks for individuals greater than $1,000 on a given day. At this point, the institution should contact the entity and communicate the need to register. Proper follow up should be done to ensure the registration is complete. If not, the institution will then have to consider its course of action – close the account, file a SAR, or both.
Indicators reflect that MSB activity risk is increasing. The Bank’s failure to identify or properly address such activity elevates the institution’s risk. This is a particular risk to community banking, due to the drive for new business and a lack of risk awareness, for which the risk indicators of a non-transparent MSB could easily be missed.

**Wire Transfers**

Wire transfers pose potential unidentified risks due to the known, stable customer base and prior successful examinations and audits. While international wire transfers pose greater inherent risk due to the unfamiliarity of foreign law in a particular country and potentially limited oversight authority, domestic wires within an institution present potential hidden risks due to an overreliance on an institution’s prior history.

The previously referenced SAR stats from FinCEN show that two separate categories of suspicious activity types relate specifically to wire transfers. These two categories rank 7th (Suspicious EFT/wire transfers) and 26th (wire transfers), which total less than five percent of filings by depository institutions from March 2012 through December 2014. The report indicates that wires are a higher risk activity. It certainly is an activity that could result in underreporting. Wire personnel often are removed from direct customer contact, whether the request comes in from an online request or from another institution location. The referrals to the BSA officer for further review and ultimate filings are often minimal. Risk is obviously reduced as many community banks are not involved in allowing wire transfers for non-customers. For those institutions that do not make use of monitoring software, the ability to review wire activities from a global perspective is at a minimum. If international wires are done on a limited basis, the tendency from a personnel perspective is to assume there is no unusual activity, but those same persons may not have a true understanding of the purpose of the wire. That understanding is even less concerning to wire personnel on an incoming wire. Training often is limited to documentation standards as opposed to the identification of suspicious activity.

Wire transfer activity can itself be a red flag, and based on the filing statistics, it is often reported as suspicious. Wire activity may be part of the usual business activities for any particular customer, but the amounts and frequencies may assist in the identification that the customer or entity should be rated higher or monitored more frequently. This becomes a significant risk in the community banking environment when the controls are not tailored to identify wire transfer risk. For example, the onboarding mechanisms might only ask whether or not the customer will be utilizing wire transfer as a product, but not require further review into frequency, threshold, or potential cross border activity of those wires. The end result might be a false sense of security that the wire transfers will be monitored effectively, whereas rules-based transaction monitoring systems need more comprehensive parameters to detect anomalous activity.

As part of the wire process, an institution should identify those originators, beneficiaries, and originating or receiving depository financial institutions on which it will perform OFAC searches.
The term OFAC search, from this point forward, is used rather generically and may include additional lists that are searched at account opening. For any transactional testing, the judgmental sampling selection should be risk based. Elevated risk would likely come in the form of international wires, large dollar amounts, in the aggregate and not solely for an individual wire, and frequency of wire activity in comparison to the account type. International versus domestic wires increases the risk because the laws and standards of the foreign country will likely be unknown to wire personnel. A sanctioned country or individual identified within any wire transfer is high risk and would require a thorough investigation of that entire relationship.

Many institutions will maintain their wire activity logs in electronic format that is easily manipulated to assist in the sample selection process. In addition to those wires selected for transactional testing, the auditor should discuss other wire activity for personnel’s understanding of the transactions for which they are processing. A log maintained that contains limited information or perhaps is handwritten limits its usefulness for efficiency for identifying higher risk transactions to sample. If the log is maintained, and international wires are indistinguishable from domestic wires, the usefulness of that log is limited. As such, the institution should maintain wire logs in an electronic, searchable format that contains sufficient information to better identify risk.

Wire transfers are a service that community banks must offer to remain competitive. The function is considered high risk from a risk of loss perspective but it is not always identified as high risk from an AML risk perspective due to many of the same factors previously identified such as a known customer base, limited products and services, and previously successful examinations and audits. The bank must not become complacent when monitoring wire transfers for suspicious activity.

**OFAC Matches**

The failure to properly assess risk or adequately perform and review OFAC searches exposes the institution to AML risk. The failure to identify positive responses results in underreporting and inadequate actions, which will result in significant regulatory consequences.

The potential failure to identify OFAC name matches (whether false or true positives) may be the result of complacency as the community bank has historically had no or very few true matches. Institutions rely on various 3rd party sources to assist in the search process. The risk exists that the 3rd party has not properly updated its list. If the search process is integrated to the institution’s systems, the list should be properly integrated into the system with the most up-to-date listing. A typographical error could result in the failure to properly search a customer even though the threshold by which systems are set will allow some error. For search results to be reliable, the individual or entity should be entered accurately, the search engine should be fully integrated and current, and the search should be conducted in accordance with the identified risk to that particular type of transaction and individual or entity. Community banks do not traditionally have matches because of their limited product and service offerings, the local customer base, and predominantly
intrastate transactions. The risk of failure increases due to complacency and the lack of attention to detail in ensuring that all methods of conducting searches are fully updated and integrated.

Many false positives are ultimately cleared and filed away. The potential match should be reviewed based on identifiable information from the search and compared to the institution’s customer information. If the results of the review result in that customer being satisfactorily resolved as a false positive, the customer may be flagged as a “Good Customer,” which is a customer that has been preliminarily screened as a potential match but that the institution clears satisfactorily upon its further review, thus alleviating the need for future reviews. The risks for failure to identify a true match result from the historical failure to have a true match requiring action on the institution’s part. The institution should identify how “Good Customers” are identified on future searches and ensure that they are included as part of the search. An appropriate audit response to this potential would be to identify a “Good Customer” and follow the process on subsequent searches to verify these customers are included. There are some basic audit procedures to perform with regards to these searches. During various sections of transactional testing – CIP and wires, for example, specific customers are tested and searches are performed in accordance with the institution’s policies and procedures. Those searches should not only be conducted in a timely manner but confirm the actual results of the search including documentation with respect to any clearing items. There are many options for sources that an institution may choose as their provider to conduct searches. Confirmation that the most recently updated list was used should be achieved. The auditor should identify the actual lists that the 3rd party provider searches. This may be communicated on the printed search documentation or may be done through inquiry with not only institution personnel but vendor documentation as well. An additional test that may be performed is to pull various names from the known list and perform the search on the institution’s systems for its OFAC searches. This should be conducted for all systems in use at the institution whether at the new accounts desk, the wire department, or the back office that may be responsible for periodic searches. Discussion with responsible parties on their knowledge of the lists actually being searched is suggested.

This process should be confirmed for International ACH (Automated Clearinghouse) transactions (IATs) and a sampling of days to confirm the review is completed and documented. A risk arises when an institution acts as an ODFI (Originating Depository Financial Institution) on ACH transactions that are “unbatched.” If those items that are not “on-us” transactions are to domestic institutions, an OFAC search may not be considered necessary. If an item is an outbound IAT, the institution should confirm the OFAC screening. The audit should confirm the extent that originated IATs are allowed, if the institution claims that is their stated policy.

The FFIEC manual states that OFAC procedures should be risk based and perhaps important to note is that “OFAC’s requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.” (19) The institution will have flexibility to determine the extent to which it conducts it searches. Personnel should be able to
discuss the reasoning for the decisions on what transactions to check, when to check, how often to check, and what lists to check. In order to prove the ultimate decision was risk-based, the decision process should be documented. Not only should the decision process documentation be reviewed so should the documentation to support the decision. As time has passed, bank personnel may not be able to reflect and identify the decisions that were made with respect to what lists we are searching, how often we are searching them, and how that was documented. Within the community banking environment, the hidden risks are presented due to complacency and overreliance, as historically OFAC and other sanctions were identified as “low” risk due to no previous matches. This risk occurs in part due to the lack of understanding as to the lists we are searching or whether our searches are conducted using up-to-date, accurate lists. In order to mitigate these risks, a clear understanding of the process should be obtained and documented.

**Politically Exposed Persons**

With respect to Politically Exposed Persons (PEPs), the BSA examination manual states, “Banks should take all reasonable steps to ensure that they do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior foreign political figures, their families, and associates.” (20) The manual also includes within this definition of PEP any entity formed for the benefit of the individual. The stated response from BSA officers is that the institution does not bank PEPs. Confirmation could be incorporated into due diligence programs; however, reliance on self-identification may not be convincing. A manual search may be impractical. If the discussion is part of the initial due diligence or ongoing due diligence with respect to the institution’s OFAC screening provider, this may be the most effective and efficient method of identifying any PEPs; however, personnel must be alert to the search process and potential existence of these parties. The complacency factor could lead to the failure to identify any change in our current customers, as historically PEPs have not been a factor. The audit should identify the process used to identify the existence of a PEP. While transactional testing is performed in other areas, the testing of PEPs can be done concurrently. If any such customers are identified, the account should be given significant consideration to being classified as high risk and subsequent monitoring performed.

For a more in-depth focus on PEP identification, the risks associated with PEPs, and performing audit tests, Alexandra Rosi’s ACAMs white paper on “How to Audit Controls to Management Financial Crime Compliance (FCC): Risks Associated with Politically Exposed Persons,” identifies several approaches to audit for the existence or identification of PEPs. The first of these advanced approaches includes the review of diplomatic passports, if available. If not available, PEPs stationed in the United States or coming for official duties are required to obtain a visa. Sampling can be achieved by sampling non-resident alien accounts. New accounts also may be sampled for account screening if the institution’s policy is to screen for PEPs with their OFAC search. Lastly, the paper references geographical locations as a potential indicator for the existence of PEPs. (21)
The potentially greater risk in banking an unidentified PEP may be the result of a long-standing customer in existence prior to the increasing intensity in which PEPs became a search criterion at account opening. For those institutions in which PEP screening is conducted at account opening concurrently with an OFAC search, the process should be confirmed and documented that the PEP search is conducted on these periodic searches. When FinCEN updates the OFAC list, it is prudent for the institution to ensure that their search provider immediately updates and conducts a search at that time. The frequency of updates to the provider’s search for PEPs should be identified. If this search process is not in place, an alternative approach will need to be considered. A manual search may be conducted although that would likely be inefficient. With respect to foreign accounts, a search of the institution’s records can identify accounts held by individuals or entities in foreign countries, which would then entail a review of the accounts of those customers and any related accounts.

For many institutions, the existence of a PEP may be remote; however, the failure to identify, or simply a poor employment of identification procedures, could result in a significant deficiency in the AML program with regards to such higher risk customers. This could be an existing, unidentified PEP but also any future PEPs that wish to open an account at the institution. Periodically, the institution should assess its processes for testing for the existence of such accounts. If there are no active measures used to identify PEPs, the institution should consider options for implementing identification methods and balance that decision based on the risk of unknown, non-compliant customer activities.

The location of the institution will influence the risk associated with the failure to identify an international PEP; however, a domestic PEP may be more likely to bank locally at a community bank in which the banking relationship began prior to political endeavors but has continued post political exposure. Additionally, a potential de-risking effect at larger institutions may exist, and the PEP may identify a community bank as a safe harbor to conduct business. As stated in the FFIEC manual, a bank should take all “reasonable” steps to ensure they do not assist in the corruption of senior political officials and their associates. In the case of a community bank, the failure to understand the risk presented based on the limited understanding of processes and procedures with respect to the identification of a PEP will not result in a “reasonable” effort to mitigate the risks in creating such a relationship. The community bank must periodically challenge its policies and procedures to ensure the failure to identify a PEP is reduced to an acceptable risk.

IV. Conclusion

The ultimate objective of any financial institution under supervision of regulatory bodies is to meet the objectives of its primary regulator to the extent that it achieves a reasonable rating with no matters requiring attention, enforcement actions, or monetary penalties. Each institution defines its own “risk appetite” with respect to this goal and implements policies and procedures to meet that end. Within the identification of that “risk appetite,” the institution may wish to enact an audit
function that provides a more thorough approach in an effort to identify unknown or previously unidentified risks within its customer base. Publicly communicated enforcement actions and penalties are the result of inadequate programs to which no financial institution is immune. The failure to properly implement policies and procedures to identify high-risk customers and activities is the greatest risk an institution will face in its AML program. The failure to identify the high-risk nature at account inception increases the institution’s risk. Subsequent identification of high-risk activities will become more difficult due to the decreased monitoring efforts for accounts not classified as high risk. Within any program, even one considered adequate or strong, the potential exists that a single, substantial oversight, such as the failure to identify a high-risk customer actively involved in money laundering or terrorist financing, could occur. Even the most experienced BSA professional runs the risk of becoming complacent or overconfident in the institution’s policies and procedures. Due diligence, a progressive control environment, and a strong audit function will be the best defense for sustainable AML success.

The AML risks in any financial institution, including a community bank, are consistent throughout the regulatory space. However, given the large degree of familiarity that community banks have with their customer bases, the misconception that their products might be lower risk, and the limited scope of some of those products, it may not be the controls themselves that fail but rather the community bank’s approach to those controls. With the absence of a strong AML risk assessment and the development of key risk indicators that may exist within the community bank’s products and services and customer base, a cursory AML audit will miss many common, hidden risks. Community banks, and by extension, AML auditors of those banks need to be able to articulate that they understand where those hidden risks may arise and that they have tailored the audit process in a way that embeds a sense of vigilance and comprehensive risk-based decision making. Thus, the community bank, through rigorous AML audits will be able to validate that those hidden risk exposures are uncovered, examined, and mitigated appropriately.

References:

(1) FinCEN, the Financial Crimes Enforcement Network. FinCEN’s Mandate from Congress. Retrieved from [https://www.fincen.gov/resources/statutes-regulations](https://www.fincen.gov/resources/statutes-regulations)


(11) United States of America, Department of the Treasury, Comptroller of the Currency. (2016, February 23). Consent Order for a Civil Money Penalty, AA-EC-


