Implementing an Effective Anti-Money Laundering System

By Kevin Harris
## Contents

- Executive Summary ......................................................................................................................... 3
- Introduction ................................................................................................................................. 4
- Choosing a Software .................................................................................................................... 4
  - 314(a) Screening ......................................................................................................................... 5
  - 314(b) ......................................................................................................................................... 5
- Currency Transaction Reporting .................................................................................................. 6
- Currency Transaction Reports Exemption ......................................................................................... 7
- Case Management ........................................................................................................................ 7
- Watch List Screening ..................................................................................................................... 8
- SAR Filing ......................................................................................................................................... 8
- Dashboard Reporting ...................................................................................................................... 9
- Cloud Computing .......................................................................................................................... 10
- IT Resources .................................................................................................................................. 10
- Testing and System Validation ....................................................................................................... 11
- Conclusion ....................................................................................................................................... 13
- Works Cited ...................................................................................................................................... 14
Executive Summary

Increased pressure from regulators have Bank Secrecy Act/anti-money laundering (BSA/AML) officers turning to software vendors for solutions which can add efficiency and accuracy to their program. Financial institutions must choose a software vendor solution that is right for their institution’s size and risk appetite. While larger financial institutions may have the ability to custom build software, many smaller institutions rely on software vendor solutions to provide them with an all-inclusive solution. This white paper should serve as a tool for BSA/AML officers who are looking to implement an automated AML software and provide real world guidance as it relates to the planning, resource, and validation stages of implementing the software. This white paper will provide insight into some of the many technical pitfalls in which BSA/AML officers commonly find during the implementation process. It will outline various tools available within most AML software, considerations to be had while implementing a new AML software, IT and staffing resources, and discuss the importance of a system validation.

Financial institutions may be looking for a comprehensive application that can perform services such as 314(a) screening, 314(b) communications, currency transaction report (CTR) filing and exemptions, case management services, watch list screening, suspicious activity report (SAR) filing, and dashboard reporting. Incorporating all of these products into one software solution can be a challenge, but if they are implemented correctly, it will help the institution ensure overall compliance with the BSA.

Financial institutions must also consider the technology resources required to take on such a project. There are advantages and disadvantages to working with software vendors who store data in the cloud. Cloud-based monitoring can free up IT resources and allow for additional cloud sharing or the institution may want to go with a server-based software which can only be accessed by their IT department for more control over safe guarding customer information. Financial institutions must carefully plan on receiving additional resources from IT as well as additional staffing in the BSA/AML department when implementing an AML software. Resources will be required during the initial implementation stage and also throughout the life of the software. With more institutions turning to automated solutions, regulators are looking to ensure that systems are validated and optimized for the best performance without missing vital data. A project of this size can take an enormous amount of IT resources to implement and institutions should be aware of the time and resources needed prior to signing the contract.
Introduction

The days of fumbling through page after page of manual reports are long gone. With today’s technology, financial institutions are expected to have an AML software in place. BSA/AML officers are required to wear multiple hats, including, but not limited, to “software specialist.” Continued scrutiny from regulators regarding AML software model validation has pushed some BSA officers to become experts at implementing and validating software. Financial institutions are looking at their AML software systems for ways to expand automation, improve performance, standardize processes and increase transparency.\(^1\) Rules-based monitoring systems are becoming less effective as criminals increase their knowledge and find new ways to commit crimes undetected. Some financial institutions are turning to a behavior-based AML solution to help predict patterns of activity indicative of money laundering and fraud activities. In addition, financial institutions are fine tuning AML software to enhance the effectiveness and timeliness of the investigative process. Financial institutions that spend time fine tuning their software will be rewarded with better quality alerts, less false positives and an overall more productive BSA program. In addition, the institution will be able to produce better quality SARs, which can help law enforcement identify and prosecute criminals. The process of finding a software solution suitable to the institution’s needs and desires can be demanding and at times can also create additional work for staff that may already be stretched thin. When determining the best AML software solution for the financial institution, it is imperative that the BSA/AML officer reviews all aspects of the AML software and determine what is essential to their institution.

Choosing a Software

When choosing an AML software solution, the financial institution must first determine the required functionality needed to complement its BSA program. Financial institutions may determine that in some instances, its system and processes in place are more than adequate and will not want to replace its current software with new technology. For example, a financial institution may find that it already screens its customer database against a multitude of watch lists and that using a new software vendor will not enhance its program. On the other hand, it may be beneficial for the financial institution to consider consolidating its systems for overall optimization. BSA/AML officers may want to weigh the benefits of consolidating systems with using the current software. Financial institutions may be looking for a comprehensive application that can perform services such as 314(a) screening, 314(b) communications, CTR filing and exemptions, case management services, watch list screening, SAR filing and dashboard reporting. Incorporating all of these

\(^1\) (Singh)
products into one software solution can be a challenge, but if they are implemented correctly, it will help the financial institution ensure overall compliance with the BSA.

314(a) Screening

The Financial Crimes Enforcement Network (FinCEN) works with law enforcement agencies to help locate financial assets and recent transactions committed by subjects of criminal investigations by using Section 314(a) of the USA PATRIOT Act. Financial institutions are required to search their records and identify individuals and entities subject to the 314(a) list. A notification is sent once every two weeks to financial institutions notifying them to log into a secure website to retrieve the list. Queries must be completed for individuals using subject and business names, addresses and other identifying records. The institution is required to review all accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last six months. Financial institutions have two weeks to complete the review and notify FinCEN via the secure website if there is a match. The 314(a) process has proven to be very efficient at combating hawala operations, arms trafficking, alien smuggling, cigarette smuggling, investment fraud, criminal networks involved in identity theft, drug trafficking rings, and healthcare and Medicare fraud.² Searching records of such proportion could be extremely intimidating and the number of false positive matches can be overwhelming if the software is not properly calibrated or does not have the capability to conduct the review. Here are some questions financial institutions should consider while implementing a new AML software provider. What information is processed through the software? Is the financial institution’s entire customer data contained within the software? Does the software provider purge closed accounts or activity after a period of time? The financial institution should feel confident that once the scan is complete that all required data was included in the search. With so many different types of criminal activity identified within the 314(a) lists, incorporating this scan into the financial institution’s AML solution could provide to be invaluable.

314(b)

Under the USA PATRIOT Act Section 314(b) financial institutions are allowed to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. Financial institutions must register with the U.S. Department of the Treasury on an annual basis.³ As stated by the

---

² (Financial Crimes Enforcement Network Department of the Treasury)
³ (United States Department of the Treasury)
Jennifer Shasky Calvery, former director of FinCEN, “A failure to share information due to systemic stove-piping, or other reasons, can significantly weaken the effectiveness of an institution’s AML program.” Some software solutions can provide financial institutions with the ability to communicate with other financial institutions using 314(b) directly through the financial institution’s AML software. Financial institutions can verify 314(b) registration, track communications with other financial institutions, and create an audit log of activity to provide to examiners when requested. Financial institutions can be notified upon request when another institution is seeking information related to a mutual customer.

Currency Transaction Reporting

The BSA of 1970 provided additional tools for law enforcement to capture illegal activity. One tool provided is the CTR. Financial institutions must electronically file a CTR for each transaction involving currency of more than $10,000. Multiple currency transactions totaling more than $10,000 during any one business day are treated as a single transaction if the financial institution has knowledge that they are conducted by or on behalf of the same person. According to recent SAR stats, one of the most common types of SARs filed is for structuring cash deposits and withdrawals. Customers who knowingly conduct transactions below the CTR reporting limit are doing so in an attempt to avoid CTR reporting. By avoiding the creation of a CTR, criminals gain anonymity and may be attempting to cover up a larger crime. Drug dealers, arms traffickers, alien smugglers and other organizations are aware of these reporting limits forcing them to operate outside of legitimate business practices which raise “red flags” for law enforcement and financial institutions. The financial institution’s AML software must recognize these red flags and create alerts to notify bank personnel of the potential suspicious activity. Some software solutions can work in conjunction with the financial institution’s core system to collect information when a person is conducting multiple transactions by or on behalf of the same person. Information is collected at the teller line about the customer’s name, address, occupation, tax identification number, etc. This information can be useful when completing a CTR or a SAR. Often times the financial institution may find that a customer who conducted multiple transactions at different locations under the cash reporting limit are involved in a structuring case already created in the software. Financial institutions should determine whether multiple businesses that share a common owner are being operated independently or if they comingle funds from one business to another in order to determine whether or not aggregation for the business is required. Some software solutions may

---

4 (The Cornerstone Report)
5 (Federal Financial Institutions Examination Council)
6 (The Cornerstone Report)
7 (Federal Financial Institutions Examination Council)
allow for the financial institutions to create groups for known associates of related entities. The system will automatically aggregate transactions based on ownership therefore ensuring the financial institution does not miss a CTR.

**Currency Transaction Reports Exemption**

Another consideration regarding the collection of CTR data is whether or not the system allows for exemptions. Under 31 CFR 1020.315(b)(1)-(5) FinCEN identifies customers who are eligible for a Phase I exemption. Phase I exemptions include banks, federal, state, or local government agencies or departments, entities whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or have been designated as a NASDAQ National market Security listed on the NASDAQ Stock Market, or any subsidiary of any “listed entity” that is organized under U.S. law and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity. In addition, under 31 CFR 1020.315(b)(6)-(7), a business not eligible for a Phase I exemption may fall under a Phase II exemption. Phase II exemptions are identified as a “non-listed business,” which is defined as a commercial enterprise to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts and that has maintained a transaction account at the exempting bank for at least two months, frequently engages in transactions in currency with the bank in excess of $10,000, and is incorporated or organized under the laws of the U.S. or a state, or is registered as and eligible to do business within the U.S. or a state. Financial institutions that allow for CTR exemption can benefit from a software that can recognize these exempt persons and omit them from filing. One way financial institutions can create efficiencies within the department are through CTR exemptions. BSA/AML officers should consider additional reporting available within the software for conducting annual reviews as well as the ability to create tasks and reminders to follow up when an exemption review is coming due.

**Case Management**

Financial institutions require a central location for building and storing case notes, attaching documents and tracking communications. One of the most critical components of an AML solution is the ability to offer a case management solution. Case management can also assist an analyst who is building an investigation. It can allow the analyst to effectively manage his/her case load by adding reminders, creating profiles, risk rating customers, and

---

8 (Federal Financial Institutions Examination Council)
ultimately filing suspicious activity reports (SAR). Maintaining good case notes throughout the SAR filing process will ensure that financial institutions are able to respond promptly to law enforcement requests and subpoenas. The ability to file SARs from the case management software is another critical component within the anti-money laundering software. It will allow the financial institution to create tasks and reminders for conducting 90-day reviews, link customers who are associates working together, and it provides analysts with a more efficient filing method. Case management may also allow the analyst to create and track tasks assigned to other individuals within the financial institution. For instance, it may be necessary to get additional information regarding a transaction in which you can assign tasks to front-line staff members to obtain the additional required information. Another advantage is that cases can be assigned or shared within a group of employees. This can be useful if the financial institution has multiple analysts working a case. Some institutions may consider combining its fraud and AML departments to allow for better communication while working cases. When information is easily shared between the BSA/AML and fraud departments, it increases the analyst’s knowledge of customer activity and allows analysts to share research data. There may be times when a fraud case turns into a money laundering situation or vice versa. In addition, both analysts get attuned to recognizing suspicious activity among all types of engagements.\(^9\)

**Watch List Screening**

Another consideration when choosing an AML software is whether or not it provides the financial institution with additional watch list screening. This may include watch lists such as the Office of Foreign Asset Control’s (OFAC) Specially Designated National and Blocked Person List, OFAC’s Non-Specially Designated National Entities List, OFAC’s sanctions screening, as well as other watch lists such as the FBI’s Most Wanted or Interpol’s Most Wanted list. The financial institution should also consider whether or not the software includes the ability to create custom watch lists. This would allow the financial institution to screen against customers on the institution’s “undesirable” list and can be beneficial to ensure that individuals or organizations who were previously determined as “undesirable” by the institution do not return. Also, it is important for financial institutions to be able to adjust the sensitivity of the watch list settings. This will affect the overall performance of the watch list screening and reduce the number of false positive alerts to review. Financial institutions should also determine if the software offers the ability to add known customers to an “accept list.”

**SAR Filing**

\(^9\) (Ernst & Young LLP)
The USA PATRIOT Act of 2001 was established to deter and punish terrorist acts in the U.S. and around the world. One way financial institutions can help to achieve this goal is by filing SARs. SARs play an important role in the detection and prevention of money laundering and other criminal activities. SAR filings can be invaluable to helping law enforcement detect crimes such as tax evasion, narcotics trafficking, human trafficking, Ponzi schemes, and many other crimes. They can help law enforcement connect the dots between criminal activity and the financial transactions that facilitate such activity. They aid not only in the detection of criminal activity but also in the prosecution of criminals. The failure to file SARs on a timely basis could impede an ongoing criminal investigation and cause financial institutions to receive criticism from regulators. Many software solutions allow the financial institution to set up alerts when SAR deadlines are coming due. This is an important consideration for BSA/AML officers when considering a software.

As the number of SAR filings increase, vendors have created a more streamlined process for filing SARs. Vendors are finding ways of making the SAR filing process more efficient through the use of templates, checklists and automation. Customer data from the core software feeds the AML software basic customer information so that the analyst does not have to recreate it in the SAR. Some vendors allow you to preview the electronic SAR form in a traditional paper based layout which can make auditing the SAR much more efficient. It is also important to have the ability to add attachments. Attachments are an efficient way for an analyst to recreate all the necessary data without having to include each transaction in the narrative of the SAR. Law enforcement can scan the narrative without sorting through pages of transactions. Once the SAR is ready for submission, the AML software can help you to submit the SAR and notify the financial institution once a Document Control Number (DCN) is received.

Dashboard Reporting

Dashboard reporting allows financial institutions to create essential reports that can assist in trending the institution’s overall risk profile. For example, if a financial institution sees an increase in high-risk customers, it may need to report the increase to senior management or the board of directors to ensure proper steps can be taken to mitigate the additional risks. The dashboard can generate reports, which can assist in creating the institution’s risk assessment. The institution can also use the reports generated to trend risky products and identify concerns. A functional dashboard can represent the geographic, product, and entity risk factors of an institution. Other risk factors such as SAR and CTR volumes, occupation/industry risk, politically exposed persons, money services businesses, and new

\[10 \text{ (Financial Crimes Enforcement Network)}\]
customer risk can also be represented in the dashboard. Charts and graphs generated from the software solution can create additional efficiencies.

Cloud Computing

Cloud computing refers to a process of sharing resources to optimize performance. Cloud computing and storage solutions provide users and enterprises with the ability to store and process their data in a third-party data center. AML software solutions can be based on cloud computing or stored and processed onsite. Both have their advantages and disadvantages. Cloud-based software providers claim that their process of storing and processing files in the cloud can enhance the customer’s satisfaction levels and enable organizations to restructure operations at a lower cost. There are many concerns with this approach related to data sharing and security. Financial institutions are concerned about the data security features of AML solutions, especially if the software is installed using a cloud-based model. There is the risk of information leaks if the data is not well protected. While there are disadvantages to cloud-based services, the market continues to grow and many AML software vendors are turning toward the cloud and leveraging additional functionality. Imagine an investigation that involves multiple financial institutions. A customer goes to Bank A to deposit $8,000 cash. The customer then proceeds to Bank B with a similar deposit of $7,000 cash. Then, the customer goes to Bank C with an additional $9,000 cash. Each individual financial institution may not alert on a single cash deposit from $7,000 to $9,000 but what if the financial institution’s AML software could see those deposits from a cloud-based network. If the financial institutions shared the same AML software using the cloud, the software provider could provide information related to all three deposits and share that information through 314(b). While the concerns of sharing information through a cloud-based system are valid, cloud-based technology has many benefits which could help put BSA/AML analysts’ one step ahead of the criminals.

IT Resources

Implementing a new automated AML software can be very labor intensive for the IT department and may require a specialist dedicated to the department which can assist in the setup and ongoing modifications required to validate and configure the new software. Due to the additional time required to test and set up a new AML software, it can be advantageous to create a project team that is knowledgeable about the financial institution’s core software and ancillary systems. Financial institutions should consider the need for ongoing support from the vendor as the financial institution will inevitably run into
initial issues as well as some that require long-term fixes. What works for one institution may not work for all. Financial institutions that use different core systems may find that integration with a particular vendor is more difficult than another financial institution using a different vendor. Therefore, the financial institution should ask questions up front to determine system compatibility.

The financial institution’s IT department can provide BSA/AML analysts with reports that can help to determine the base settings for the financial institution’s AML software. Reports may include the average ACH, wire, cash, and check activity conducted by your business clients as well as the averages conducted by the financial institution’s personal clients. The averages can be used to help determine configuration settings as the initial settings set by the vendor may not be ideal for your institution. Settings can also be adjusted to the level of risk associated with the financial institution and determined in the institution’s risk assessment.

Once the new AML system is up and running, the financial institution will need training for staff. It is important to know what kind of support and training will be available from the vendor prior to signing the contract. Is the training online, in person, or a combination of both? Perhaps the vendor offers some additional support through a help line. Are there additional costs associated with calling in for guidance? If the financial institution requests for additional reports to fulfill a need, can the vendor supply it?

A best practice when implementing a new AML software is to run both the financial institution’s pre-existing system and its new AML software in tandem for a period of time to adjust and configure the settings as well as to ensure additional issues are identified prior to going live. This will also provide insight to the volume of alert activity to anticipate and allow the institution to determine additional staffing needs to meet the demands of the new system.

Testing and System Validation

One of the most important phases of implementing a new AML software is testing and system validation. An industry best practice is to validate that data transmitted from the core is correctly received by the AML software and that alerts are performing as expected. Financial institutions may consider outsourcing this testing to a third party as this will inevitably be looked at by the regulators. System validators may perform a series of tests to ensure overall efficiency and accuracy. One type of analysis that can be performed is transaction code mapping. This process verifies that all transaction codes from the core banking system are properly mapped and coded to the AML system. Another type of verification is alert processing validation. This process involves an analysis of the
configuration of the automated systems alert engine. A third type of validation is transaction coverage verification. This process involves the extraction of a sample of core transaction data and automated monitoring system transaction. The data from the core system is reconciled to a corresponding period of automated monitoring system data to determine if there are any gaps.\textsuperscript{11} Sample sizes should be commensurate with the financial institution’s overall size. As a best practice, the validation process should be conducted on an annual basis. This validation process not only complies with regulatory expectations but also acts as a vital control in a BSA program.

When planning for validation testing, financial institutions should consider the following:

- Technical and regulatory knowledge of staff
- Access to tools and support to conduct the testing efficiently and accurately
- Data integrity testing
- Careful consideration of the data tested to ensure replication of the production environment and complete coverage of sufficient date ranges
- Maintain a complete documented process\textsuperscript{12}

Another consideration regarding system validation is adjusting the AML software’s sanctions screening configurations and settings. The financial institution will want to configure its settings to match the overall risk appetite of the financial institution and according to its risk assessment. Settings within the software should allow financial institutions to customize the alert hit rate as well as the countries included in the sanctions screening. Many filters contain every name on OFAC’s list of Specially Designated National and Blocked Entities along with generic words for countries and cities. When the system identifies a potential match, the analyst is notified to review the alert.\textsuperscript{13} OFAC scanning software should contain an accept list to help manage the number of false positive alerts the financial institution receives. An “accept list” will prevent the software from reporting matches for the same entities that you have already determined to be false positives in previous searches. It is also important to ensure that your software will alert you in the event that any meaningful changes to the customer’s information (e.g., a change in ownership status, business activity, address, date of birth, place of business, etc.) triggers a review of the “accept list.”

\textsuperscript{11} (Lutz) 
\textsuperscript{12} (Protiviti) 
\textsuperscript{13} (The Department of the Treasury)
Conclusion

Today’s AML software systems offer a variety of components to automate processes such as 314(a) screening, 314(b) communications, CTR filing and exemptions, case management services, watch list screening, SAR filing and dashboard reporting. It is imperative that BSA/AML officers conduct due diligence when looking for a software provider to understand the tools that are available to assist them in enhancing their BSA program. Financial institutions should consider the time and resources required to implement the system as well as staffing requirements to maintain a well calibrated software solution. Once properly integrated and calibrated, an automated AML solution can increase alert efficiency and accuracy.

Failure to comply with BSA regulations can have serious consequences, which can result in both civil and criminal penalties. In addition, the financial institution can face public embarrassment, which can affect the institution’s reputation and bottom line. Along with satisfying the regulatory requirements, systems must also be flexible and continue to evolve as criminal activity continues to evolve and new products are released. Software vendors must be diligent in staying on top of new regulations and trends in order to provide analysts with the most up-to-date tools. Law enforcement depends on CTR and SAR information provided by the financial institutions to identify and prosecute criminal activity. Ultimately, it is the financial institution’s responsibility to ensure that its BSA/AML department is compliant and financial institutions must perform a fair amount of due diligence on vendors prior to entering into a long-term relationship.
Works Cited


