AML COMPLIANCE GUIDE

5 Keys to Streamline Your AML Program

The perennial fight to detect and prevent financial crimes, such as fraud, money laundering and identity theft, can be frustrating and exhausting to businesses on the front lines of that war. After all, the enemy is well armed, opportunistic and constantly evolving to improve its efficiency and success rate. Financial criminals aren't afraid to embrace the latest technology and modern tactics to capitalize on changing societal landscapes and trends. This gives them a distinct advantage in the anti-money laundering (AML) battle. The only way to thwart them is by modernizing and streamlining your own AML efforts.

AN AML COMPLIANCE OVERVIEW

As part of the U.S. Treasury Department, the Financial Crimes Enforcement Network (FinCEN) is responsible for issuing regulations under the Bank Secrecy Act (BSA), which requires financial institutions to establish a BSA/AML program[1] that includes:

- A system of internal controls to ensure compliance
- Independent testing of the program
- A designated BSA compliance office or officer
- BSA/AML training for all appropriate staff
- A customer identification program (CIP)
- Ongoing risk-based customer due diligence (CDD), including for legal entity beneficial ownership[2]

WHO IS RESPONSIBLE FOR COMPLYING WITH AML?

After the attacks of Sept. 11, 2001, the USA PATRIOT Act expanded the definition of financial institution beyond traditional banks to include other industries that face a higher risk of money laundering and sanctions screening violations. The following entities, which include those using financial technology to offer and provide bank-like products and services, must have adequate AML safeguards in place:

- Automobile, boat and airplane dealers
- Casinos and gaming establishments
- Charities and non-profits
- Depository institutions
- Insurance companies
- Money services businesses (MSBs)
- Mortgage companies and brokers
- Precious metal and gem dealers
- Securities, commodities and futures brokers and dealers
- Travel agencies

Traditional banks and other industries facing a higher risk of money laundering and sanctions screening violations must have adequate AML safeguards in place.

MODERNIZE YOUR AML COMPLIANCE

In order to meet BSA obligations, financial institutions typically divide their AML program into four distinct task areas:

1. CIP identity verification to ensure know-your-customer (KYC) compliance
2. AML monitoring to uncover potential suspicious activity
3. Real-time fraud monitoring to stop illegitimate or unlawful transactions
4. Sanctions screening to prevent doing business with anyone designated on watchlists

Over the years, depending on their risk profile, size and sophistication, financial institutions have used a variety of manual and software-based processes to tackle these AML tasks with varying degrees of success. Given the ever-quickening pace at which financial criminals elevate their own technology and tactics, today's financial institutions need to do more to stay ahead.

Here are five ways to modernize your AML program to meet regulatory requirements and protect your institution and its customers from financial crime:

KEY 1: CONDUCT AN IN-DEPTH RISK ASSESSMENT

A current and comprehensive risk assessment should form the foundation of your AML program. This exercise must thoroughly answer questions such as:

- **Where is your institution most at risk?** This can change over time. New products or geographic markets can alter your risk profile, as can external events like the COVID-19 pandemic.
- **What are the weakest parts of your AML program?** For instance, through your risk assessment, you may discover that your fraud monitoring is successfully preventing illicit transactions but your sanctions screening program is inadequate and needs attention.
- **Where are you spending the most money in your AML program?** If your AML budget allocations aren't prioritized from highest to lowest risk, your program isn't cost efficient or effective at preventing financial crime or subsequent regulatory fines.
- **Are your AML systems and models effective?** As indicated by the Interagency Statement on Model Risk[3], a sound risk management approach should be used to evaluate the safety, soundness and compliance effectiveness of any systems or models being used for AML compliance.

Once your risk assessment is complete, you can figure out where to appropriately adjust and update your AML program for more cost and compliance effectiveness. Financial institutions should conduct a risk assessment on an annual basis and any time there is a significant internal change, such as a product rollout, or an external event or trend that alters the risk landscape.

KEY 2:
EMBRACE AUTOMATION AND MACHINE LEARNING

The biggest AML expense at smaller financial institutions is typically compliance staff. Without the help of technology, it takes more people to detect and prevent financial crime—an expensive method that ultimately struggles to thwart criminals who constantly revise and evolve their tactics. However, today's cloud-based solutions can automate many of the tedious and time-consuming tasks associated with AML compliance, and such platforms can be configured to meet specific institutional needs. This leaves AML staff to concentrate their efforts where human interaction is most needed and useful.

A lot of early AML software was rules-based, which meant that once financial criminals figured out the rules, they could devise ways to get around them. But the latest automated solutions introduce artificial intelligence (AI) and machine learning (ML) into AML efforts, making them dynamic and harder for criminals to evade.

These next generation AML platforms learn with each new activity or transaction, creating fuller and clearer customer profiles the longer they're used. As a result, it's easier to differentiate between genuine and suspicious activity, identify hidden threats and focus AML efforts and budgets where they are most needed. This adds a significant boost to AML programs, in particular for larger institutions that devote a significant amount of valuable human resources investigating false positives.

The latest automated solutions introduce artificial intelligence and machine learning into AML efforts, making them dynamic and harder for criminals to evade.

KEY 2:
EMBRACE AUTOMATION AND MACHINE LEARNING *(continued)*

With transaction monitoring for example, as the machine learning technology continuously sifts through large sets of operational, compliance and external data in real-time, it gains a truer understanding of what constitutes risky or anomalous behavior for any given customer, enhancing its ability to detect true suspicious or fraudulent activity. This includes:

- Using intelligent pattern identity to distinguish between a rare transaction type that is legitimate and one that is not
- Scouring across customer data to uncover previously unknown suspicious activity
- Performing a deep analysis of customer activity that reveals previously opaque or layered transactions for potential fraud

As for sanctions screening, machine learning technology allows for a more nuanced search of customer names, including the order of names, titles, salutations, abbreviations, name variants and common misspellings.

Institutions can choose an all-in-one platform that handles all four AML task areas or invest in a solution that deals with one or more specific AML tasks that their risk assessment identified as particularly hazardous or weak.

KEY 3:
CLARIFY AND SIMPLIFY PROCESSES AND PROCEDURES

Investing in next generation AML automation can be a game changer for financial institutions, but it can also disappoint if you don't likewise invest the time to review and update your written processes and procedures to make sure that they:

- Incorporate the latest AML best practices
- Match what actually occurs in your institution
- Provide clear and consistent direction to staff
- Reflect any and all automation in use

KEY 4:
CONFIGURE AML TECHNOLOGY TO YOUR NEEDS

Every institution's risk profile is different, which is why it is crucial to explore all the features, functionality and customization options available when scouting out automated AML solutions. For instance, investigate the following:

- **Does the solution handle one, several or all AML task areas?**
- **What type of reporting and audit trail does it generate?**
- **How does it integrate all of your internal data (customer risk profile, customer transactions, historical suspicious activity, etc.) and external data (company website and socials, industry databases, news reports, etc.) in order to analyze and learn customer behavior?**
- **How easy is it to adjust assumptions or models for continuous enhancement of your AML efforts?**

But that's only the first step. Once you select a solution, you need to actually configure it based on your needs, and document that configuration for regulatory examination purposes. Your solution provider should supply you with a written explanation of how their platform works, which can form the basis of your documentation, but examiners won't consider it sufficient if it doesn't reflect how your institution uses the system in reality.

KEY 5:
ADEQUATELY STAFF YOUR COMPLIANCE OFFICE

Technology is now a necessary and crucial part of AML compliance, which means that compliance staff need to be tech savvy enough to:

- **Help configure the system at implementation based on your risk assessment and processes**
- **Adjust its configuration when risk assessments reveal changes in the threat landscape**
- **Document its use and explain how it works to regulatory examiners**
- **Create appropriate audit trails**

Your solution provider should offer support and training to help your staff gain this needed knowledge and comfort. However, on your end, AML compliance staff job descriptions should be updated to adequately reflect your institution's level of reliance on AML technology and require a corresponding proficiency in the same.

Your solution provider should offer support and training to help your staff gain this needed knowledge and comfort.

WHAT'S THE TRUE COST OF AML COMPLIANCE APATHY?

Financial institutions that fail to modernize and streamline their AML compliance programs face a number of potential financial consequences. The most obvious is falling victim to financial crime. PwC's 2020 Global Economic Crime and Fraud Survey[4] revealed that 56% of respondents representing U.S. companies experienced fraud in the past 24 months for a total of $6.5 billion in fraud-related losses.

There is also the genuine risk of regulatory fines. Here's a snapshot of recent BSA/AML-related civil money penalties[5]:

- $390 million to a traditional bank
- $60 million to the CEO of a bitcoin-related firm
- $38 million to a securities firm
- $22.5 million to a gaming establishment

In addition to the revenue impact of falling victim to financial crime or receiving a regulatory fine, financial institutions face reputational harm as a result of both of these circumstances.

Finally, there's a cost to not aligning AML technology investments to your actual needs. If you select an automated AML solution without first understanding what you require, you risk one of two things: paying too much for a system that provides more than you need versus paying too little for a system that leaves gaps to be back-filled by labor-intensive manual processes or additional technology.

Given the relative affordability and AI-embedded sophistication of today's AML solutions, there's no need to cede the AML battle to financial criminals and every reason to take the fight to them.

ABOUT CSI

As a trusted partner in the regtech industry, CSI provides regulatory compliance software and services to thousands of customers worldwide, helping them stay compliant with today's top federal regulations, including OFAC, USA PATRIOT Act, GLBA and more. CSI's advanced compliance software solutions employ the latest technology to automate and streamline denied party screening, filing and fraud prevention to improve risk management and protect business integrity. As a compliance partner, CSI's innovative solutions help minimize false positives, reduce labor costs and strengthen practices in the face of rapid regulatory change. Visit www.csiweb.com for more information.

RESOURCES

[1] BSA/AML Program

[2] Legal Entity Beneficial Ownership

[3] Interagency Statement on Model Risk

[4] PwC's 2020 Global Economic Crime and Fraud Survey

[5] BSA/AML-Related Civil Money Penalties