AML INTEGRITY

The Foundation of Our Homeland Security

The Bank Secrecy Act was passed by the United States Congress about a half-century ago. Before the year 2000, a violation of AML compliance would only expose a financial institution to a relatively minor regulatory penalty. Because fraud losses could cost a financial institution much more money than the penalties paid for AML violations, quite a number of financial institutions used fraud prevention products to handle both fraud monitoring and AML monitoring to save money and time. That reckless practice imperiled our homeland security.

After President George W. Bush signed the USA PATRIOT Act on October 26, 2001, the U.S. government regulators invested a tremendous amount of resources to educate their examiners on the differences between AML monitoring and fraud monitoring. At that time, a financial institution could receive a huge regulatory penalty when it used a fraud monitoring method for AML monitoring. A true AML expert would never use a fraud monitoring method for AML monitoring.

Unfortunately, the mortgage crisis broke that AML compliance momentum because government regulators needed to shift their resources to supporting the fragile economy. Additionally, many experienced AML professionals changed their roles due to promotion, retirement, or reallocation of resources. Take a guess at what is happening now…

History is Repeating Itself

Many financial institutions are again using fraud monitoring methods for both fraud monitoring and AML monitoring. Sadly, even some auditors cannot tell the differences between fraud monitoring and AML monitoring. In order to sell fraud prevention products under the disguise of AML compliance, those vendors hide their flaws with false claims. Below are some examples.

False Claim #1

Some vendors falsely claim that financial institutions can jointly prevent fraud based on Section 314(b) of the USA PATRIOT Act. Some novices in the industry even believe this false claim to be true.

FinCEN has repeatedly stated that Section 314(b) can only be used for Anti-Money Laundering and Counter Terrorist Financing purposes, and Section 314(b) cannot be used for fraud prevention purposes. **In fact, FinCEN has specifically stated: "An entity that participates in the 314(b) program and that fails to maintain appropriate procedures to ensure compliance with the requirements stated in 31 CFR § 1010.540(b) may be subject to penalties."**

False Claim #2

Some vendors falsely claim that money laundering always occurs after fraud and detecting fraud is the same as detecting money laundering. This claim is false. For example, when a fraudster uses a victim's credit card for a shopping spree, there is no money laundering activity at all. For most fraud cases detected by financial institutions, such as check fraud, credit card fraud, debit card fraud, ATM fraud, ACH fraud, wire fraud, etc., the customers in these fraud cases are "victims" of the fraud and are not money launderers. **Experienced examiners can easily tell that a financial institution is using fraud monitoring methods for AML monitoring when fraud alerts are mixed together with money laundering alerts.**

False Claim #3

Some vendors falsely claim that their systems can use behavior changes to detect money laundering and fraud at the same time. In reality, their systems have missed many true money laundering cases because money laundering can be conducted without any behavior change. For example, a human trafficker can routinely send funds to a remote accomplice without changing behavior. To cover up their flaws, those flawed products are designed like a black box, hiding the reasons for triggering alerts. **Experienced examiners can easily determine that a financial institution is not conducting AML monitoring when its AML system cannot explain the reason for triggering an AML alert.**

False Claim #4

Some vendors falsely claim that their systems only need to monitor transactions over a short period to detect money laundering activities. The flawed products are designed to fool examiners by *showing repeated alerts* when the products show the detection results over a longer period. The reality is that these flawed products cannot monitor transactions structured over a long period. A true AML expert knows that money laundering can be structured throughout a long period of time, such as once per quarter, etc. **Experienced examiners have already established that a financial institution has missed the basic money laundering cases when its AML system cannot conduct data mining over a long period.**

False Claim #5

Some vendors falsely claim that their systems only need to monitor accounts, not relationships. A true AML expert knows that a financial institution needs to monitor related customers because they can jointly conduct money laundering. **Experienced examiners have already concluded that a financial institution has missed many money laundering cases when related customers are not monitored together.**

Some foreign vendors do not truly care about U.S. homeland security. Those foreign vendors know very well that they are actively cheating U.S. government examiners and U.S. financial institutions when they use fraud monitoring methods for AML monitoring.

For our fellow Americans who still remember what we endured during the difficult early 2000s, let us conscientiously unite together to ensure that no financial institution will use fraud monitoring methods for AML monitoring to endanger our homeland security again.

AI OASIS