THE RIGHT WAY

Are False Positives Wasting Your Time Every Day?

Many BSA Officers have voiced their common frustration of wasting time on false positives every day at the expense of detecting actual money laundering cases. This frustration is the result of an old misconception promoted by some software vendors, who claim that their software packages can detect money laundering cases and fraud cases at the same time because money laundering and fraud always occur together. After purchasing such software packages, the users try to detect fraud cases and treat the victims of fraud as money launderers. As a result, the financial institutions have wasted a huge amount of time, money, and resources.

This misconception can be corrected through a proper understanding of the sophisticated facets of transactional risks. Transactional risks are defined as risks directly associated with the transactions. For example, money laundering risk and fraud risk are directly associated with the transactions. Nevertheless, these risks possess very different characteristics. Customers who conduct money laundering through financial institutions intend to use the financial institutions as vehicles to achieve their goals. These money launderers usually pretend to be “good customers” because they need the financial institutions’ assistance to accomplish their money laundering schemes. They do not mind paying extra fees or losing interest on their money, and thus from the financial institutions’ perspective, these money launderers may appear to be desirable customers to have. This is a key reason why financial institutions need to conduct data mining on all transactions in order to identify money launderers, who appear to be “good customers.”

In comparison, fraud risks manifest themselves very differently. Fraud cases associated with financial institutions can be generally classified into two categories: (1) third-party fraud and (2) counter-party fraud. For example, both the financial institution (i.e. primary party) and the customer (i.e. counter party) are victims when a fraudster (i.e. third party) steals a checkbook from the customer. Under such circumstances, the transactions conducted by the third-party fraudster have nothing to do with the customer. It is therefore a waste of time, money, and resources when the fraud detection product misleads the BSA Officer to assume that the customer has conducted money laundering.

For counter-party fraud, once the customer has successfully cheated a financial institution, the customer will quickly disappear and use another financial institution to launder the stolen money. It is a fraud case to the first financial institution, but a money laundering case to the second financial institution. These are two different types of crimes occurring in two different financial institutions.

In reality, **money-laundering cases and fraud cases often occur independently.** For example, when a fraudster uses a victim’s credit card to conduct a shopping spree, although there is a behavior change, there is no money-laundering activity at all. **The customer is actually a victim of fraud, not a money launderer.** Similarly, when a drug dealer sends money through a financial institution to buy drugs, there is no fraud activity at all. This is the reason why FinCEN’s Suspicious Activity

Report (SAR) form clearly distinguishes between money-laundering activity and fraud activity. **A financial institution will miss countless money-laundering cases if it uses fraud detection methods to detect money-laundering activity.** Clearly, a software product that intends to detect fraud cases every day will systematically create many false alerts for money laundering and actually miss the real money laundering cases. Using such a faulty product will increase the workload of the BSA Officer and expose the financial institution to unnecessary regulatory risk.

There are many different types of fraud cases and a good transactional risk management system must use multiple detection engines that intelligently take into account each unique characteristic of the various fraud risks. Because a financial institution needs to stop fraud as soon as possible to prevent losses, a fraud detection system should detect fraud as close to real time as possible, or at least once daily. By contrast, because multiple customers may launder money or finance terrorists together by conducting one small transaction per person on different days, daily monitoring will miss such cases. For this reason, money laundering and terrorist financing activities must be monitored by a different detection engine, which conducts data mining on all transactions of the entire financial institution accumulated over a longer period of time. **This leads to the logical conclusion that a product, which intends to detect fraud cases and money laundering cases at the same time, will waste resources and miss true money laundering and terrorist financing cases.**

PATRIOT OFFICER uses multiple detection engines running at different speeds to monitor transactions and seamlessly integrate the detection results into a centralized case management platform. This approach effectively consolidates and streamlines the Anti-Money Laundering and the Anti-Fraud processes with maximum efficiency, while maintaining a holistic, accurate picture of each customer at all times. As a result, PATRIOT OFFICER empowers a financial institution to:

- comply with laws and regulations;
- eliminate both money laundering risks and fraud risks;
- avoid losses and damages;
- minimize resources in managing transactional risks;
- reduce costs associated with hardware, database, and software;
- lower IT maintenance workload; and
- increase the overall productivity and profitability of the financial institution.

Publisher Background

GlobalVision Systems, Inc. is the largest independent provider of regulatory compliance, risk management and fraud prevention solutions in the U.S.A. It has produced the renowned PATRIOT OFFICER®, GUARDIAN OFFICER®, and ENQUIRER OFFICER® and has established the de facto standards for BSA/AML compliance in the USA. For more information, please contact sales@gv-systems.com or (888) 227-7967.