Are False Positives Wasting Your Time Every Day?

The Intelligent Way to Consolidate Anti-Money Laundering and Anti-Fraud Resources

At a recent Anti-Money Laundering (AML) conference, many BSA Officers voiced a common frustration that they were wasting time on false positives every day at the expense of detecting actual money laundering cases. This frustration is the result of a prevailing misconception that has been promoted by some software companies who claim that money laundering and fraud are often crimes committed by the same offender and should be detected together by using their software packages. After purchasing such software packages, some financial institutions try to detect both money laundering cases and fraud cases together. This has resulted in a huge amount of time, money and resources being wasted.

This misconception can be corrected through a proper understanding of the sophisticated facets of transactional risks and by using a solution that truly helps financial institutions consolidate their resources to easily, effectively and efficiently manage these 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” since they need the financial institutions’ assistance to accomplish their 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 great customers. This is a key reason why financial institutions need to conduct data mining on all transactions in order to detect money laundering activities which are hidden behind the scene.

In comparison, fraud risks manifest themselves very differently. Fraud committed by customers can be generally classified into two categories: (1) third-party fraud and (2) counter-party fraud. Third-party fraud is defined as fraud committed by a third party that is not the financial institution and is not the customer. For example, both the financial institution (i.e. primary party) and the customer (i.e. counter party) may become 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 BSA Officers are misled by an ineffective software product to assume that a customer has conducted money laundering simply because the customer is a victim of fraud committed by a third party.

Counter-party fraud is defined as fraud committed by a customer (i.e. counter party) who cheats the financial institution (i.e. primary party). Once the customer has successfully cheated the financial institution, the customer will quickly disappear and will not conduct money laundering through the financial institution. Clearly, a software product that intends to detect fraud cases every day will systematically create many false positives for money laundering and actually miss the real money laundering cases. Using such a faulty product will increase the workload of the BSA Officers and expose the financial institution to unnecessary regulatory risk.

There are many other risks under the category of third-party fraud worth noting. For example, counterfeit check, credit card fraud, debit card fraud, ATM fraud, online fraud, etc. are typical risks under the category of third-party fraud. Similarly, there are many different risks under the category of counter-party fraud, such as check kiting, deposit fraud, loan fraud, etc. Therefore, a good transactional risk management system must use multiple detection engines that intelligently take into account each unique characteristic of the various fraud risks in order to successfully detect fraud. Furthermore, as illuminated in the white paper "BSA Red Flags," multiple customers may launder money or finance terrorists together by conducting one small transaction per person on different days, and daily monitoring will miss such cases. For this reason, money laundering and terrorist financing activities must be detected by a different detection engine which conducts data mining on all transactions of the entire financial institution accumulated over a period of time. This leads to the logical conclusion that a product using a single engine to detect fraud, money laundering and terrorist financing activities together will waste resources and miss true money laundering and terrorist financing cases.

The correct approach to managing transactional risks is to utilize multiple detection engines monitoring transactions at their own speeds and to seamlessly integrate them into a Centralized Case Management Platform. This approach effectively consolidates and streamlines AML and Fraud Prevention with maximum efficiency while maintaining a holistic, accurate picture at all times. As a result, a financial institution can efficiently comply with the regulatory requirements, eliminate risks, avoid losses, boost productivity, minimize resources in managing transactional risks, reduce costs associated with hardware, database and software, lower IT maintenance workload, and increase the overall profitability.

In summary, the following guidelines serve as the best practice to consolidate the resources in transactional risk management:

- Use multiple detection engines to monitor different transactional risks
- Monitor various fraud risks at least daily or as close to real-time as possible
- Monitor money laundering risk through data mining of all transactions accumulated over a period of time
- Use a Centralized Case Management Platform to fully integrate the above detection engines while consolidating AML and fraud prevention resources with maximum efficiency
- Share hardware, database, software and human resources whenever possible

Author Background

Mr. Oliver Song is the Chief Executive Officer of GlobalVision Systems, Inc., which has produced the well-known PATRIOT OFFICER®, GUARDIAN OFFICER®, and ENQUIRER OFFICER®, all of which share a Centralized Case Management Platform as illustrated in this white paper. Mr. Song holds over 10 patents and pending patents and is a well-respected top expert in the regulatory compliance, risk management, and fraud prevention software industry. For more information, please refer to www.gv-systems.com.