Why Your Bank Is Better Off With Fewer Fraud Alerts

4 Ways to Combat Fraud More Effectively

As the cost of cybercrime escalates across all industries, banks are suffering the most: According to a study from the Ponemon Institute and Accenture, the cost of cybercrime in the financial services industry is $18.37 million a year – more than any other industry. This rise in fraud translates into an avalanche of fraud alerts with the potential to inundate and overwhelm banks and their fraud investigators.
The sheer volume of alerts, especially false-positives, can take time and attention away from analyzing and understanding the patterns that underlie costly fraudulent activity, including insider, payments systems, and cross-channel fraud as well as money laundering. Instead of focusing on reacting to alerts, banks should adapt technology and techniques aimed at placing alerts in context and allowing for proactive management of those alerts.

A four-step systematic approach to reducing alert volume, segmenting alerts, and managing alerts can lower your institution's overall risk profile. Such an approach has the potential not only to stem losses from fraud, but also to stop fraud at its source – shortening case cycle time, improving the quality of investigations, and maximizing the productivity of network operators and fraud investigators.

WHERE DO ALL OF THESE ALERTS COME FROM?

Leading fraud solutions incorporate deep layered security that reduces fraud risk by generating alerts that identify suspicious and unusual activity.

1. Look at past data trends in order to identify known 'bad behaviors' in a quick and efficient manner.

2. Understand what's normal behavior for an employee based on their past actions and the actions of those in similar roles.

3. Identify hidden insights and patterns in transactional and user data while utilizing investigator feedback to consistently refine filter and scoring systems.
Instead of focusing on reacting to alerts, banks should adapt technology and techniques aimed at placing alerts in context and allowing for proactive management of those alerts.
Reduce Alert Volume

Alerts represent potential risks to your institution. Placing alerts in context by assessing business risk reduces the number of alerts. When evaluating alerts, a business risk mindset considers:

- Amount of potential revenue loss
- Negative impact on reputation
- Possible compliance or legal ramifications
- Potential loss of intellectual property
- Effect on the institution’s competitive position

To detect fraud, a filter and scoring system generates fewer alerts but prioritizes high-risk transactions that have a significant likelihood of being fraudulent. Risk-based filters categorize and classify alerts. Then a scoring system evaluates the potential likelihood of fraud and the potential magnitude of fraud for a given transaction and ranks alerts accordingly.

It is critical to understand, however, that the accuracy of such a scoring system and its efficacy in reducing the number of false-positive alerts is increased by obtaining and correlating data from multiple channels – applications, systems, networks, and log files – to reveal risky patterns. A risk score that relies solely on the information from one application interaction or data set may not reflect the true risk involved.

In action, an effective scoring system would, for example, rank alerts around the potential infiltration of bank systems by a sophisticated network of hackers far higher than a simple individual check fraud. This ability is critical because hackers constantly innovate. No institution is immune to large-scale fraud.

Leading solutions leverage machine learning models to consistently update the scoring system based on deftly identified data points, including the results of past investigations.

PRIORITIZING HIGH-RISK TRANSACTIONS

Data correlation and analysis reveal that the three alerts in combination result in a high-risk score demanding immediate investigation.
Segment Alerts to Prioritize Actions

Investigation teams possess a finite amount of time and energy. Implementing a system that segments alerts by category introduces more efficiency into the system.

Without segmentation, you might simply take the top 100 alerts based on their risk score. The problem is that some alerts that deserve your attention may not make that list. For instance, what if an alert signifying a possible money-laundering episode is buried further down the list? Segmenting allows you to prioritize certain types of alerts over others – such as a million dollar wire transfer fraud over a single incidence of mobile deposit fraud – to appropriately address business risk. You may want your investigators to review every alert from one category but only the top 10% from another.

By evaluating the business risk associated with each segment and combining that information with the risk scores for the alerts, you can determine which alerts should claim priority processing each day. You can further improve this segmentation by utilizing machine learning models to refine the risk scoring process within each segment you define. This context specific scoring helps investigators move away from a mindset focused on speed toward a mindset focused on risk management and the best ways to protect the interests of the bank.

Segmenting allows you to **prioritize certain types of alerts over others** – such as a million dollar wire transfer fraud over a single incidence of mobile deposit fraud – to appropriately address business risk.
Consider the skill, complexity, and time involved in a typical fraud investigation. An investigator needs to understand what different data points mean, identify the important pieces of data for a given alert, cross-check other systems for confirmation, establish connections between data points, and more.

Maximize Investigator Productivity

While scoring and prioritization help investigators focus on the most important alerts, your bank will also benefit from a system that improves investigator productivity. To increase both the speed and accuracy of investigations, look for a system that can do the following:

- **Give investigators a complete picture of the situation.** Look for a tool that can consolidate information to alleviate the need to maneuver between different systems and contextualize it to give meaning to raw data points.

- **Speed investigations by managing workflow.** An investigation may need to follow a compliance process or have input from multiple departments, such as human resources, legal, or finance. But when a file moves to the next person, it can get lost in transit. A good workflow tool tracks each case from initiation to conclusion, sending reminders when necessary to keep a file moving and providing management with complete visibility into the caseload.

- **Provide advanced search capabilities.** For instance, investigators may know that insider fraud has been perpetrated on a certain account, but not know how or by whom. A Google-like search can help them quickly find what they are looking for. Screen-by-screen replay can then give them visibility into every activity that has taken place for that account along with who performed the activity step-by-step. They can then determine if a single employee was involved in the fraud or if employees acted in collusion, as well as if the fraud was an isolated incident or part of a larger pattern.

When bank fraud investigators are armed with the tools to manage cases more efficiently and effectively, they stand a better chance of stopping fraud before a bank sustains significant and ongoing losses.
When bank fraud investigators are armed with the tools to manage cases more efficiently and effectively, they stand a better chance of stopping fraud before a bank sustains significant and ongoing losses.
Lower Your Bank’s Risk Profile

Improving the management of fraud alerts is critical to protecting a bank’s revenue stream, reputation, compliance position and customers. A filter and scoring system that translates fraud alerts into business risk and appropriately scores, categorizes, and segments them enables you to reduce the number of fraud alerts and identify the top priorities for your investigation team. As a result, investigators can concentrate their efforts where they can have the greatest impact on your bank’s risk profile. Using a filter and scoring system, along with other tools that can shorten case cycle time and improve the quality of investigations, will enable your institution to manage fraud alerts efficiently and with confidence.

Is your cyber fraud and risk management solution able to stand up to the evolving threat landscape? Find out how you can stay ahead with this informative video.

Learn how Bottomline Cyber Fraud and Risk Management solutions can help you detect internal fraud, employee account takeover, and data leakage.

CONTACT US

Improve the management of fraud alerts is critical to protecting a bank’s revenue stream, reputation, compliance position, and customers.

About Bottomline Technologies

Bottomline Technologies (NASDAQ: EPAY) helps make complex business payments simple, smart, and secure. Corporations and banks rely on Bottomline for domestic and international payments, efficient cash management, automated workflows for payment processing and bill review, and state of the art fraud detection, behavioral analytics and regulatory compliance solutions. Thousands of corporations around the world benefit from Bottomline solutions. Headquartered in Portsmouth, NH, Bottomline delights customers through offices across the U.S., Europe, and Asia-Pacific.

For more information, visit www.bottomline.com