Bottomline

The Threat from Within: Defending Your Organization against Internal Fraud

A recent survey by Themis indicates that 74% of banking professionals are concerned about the insider fraud and collusion risks facing their organization[1]

Additionally, 85% of institutions reported that they lacked insider fraud tools to detect internal fraud or have outdated systems and controls that are not effective enough.

PROFILES OF INTERNAL FRAUDSTERS

Threats from insiders—employees or partners—aren't uncommon and they shouldn't be discounted. These can come from several sources:

- **Inside Agent** – a person who steals information on behalf of criminals on the outside in return for a bribe or money
- **Disgruntled Employee** – an unhappy employee who uses assigned credentials to intentionally destroy data or to harm the organization
- **Malicious Insider** – a person who steals data from a company for personal gain, by using existing privileges to gain access to systems and data
- **Careless Worker** – an employee who unintentionally breaks policies, mishandles data or installs unauthorized applications
- **Third-Party** – a trusted vendor or an associated application that compromises data security, whether intentional or not

To protect itself and its customers against insider attacks, organizations must put fraud prevention measures in place and regularly evaluate performance. Education and training can go a long way to combat accidental data compromise but it's harder to identify intentional insider fraud by employees who have access to

Organizations on average lose

5%

of their revenue to internal fraud each year. A typical internal fraud case occurs for 14 months before it is detected.[2]

1. Themis, Insider Fraud in Banks – Post-Covid Threat Landscape, 2022
2. ACFE Report to the Nations, 2021

Case Study

As part of an ongoing security evaluation, one national bank decided to audit its existing, legacy behavior monitoring solution that tracked internal account activity. The bank discovered that the process in place, although effective, was highly-customized which made it difficult to scale and modify the technology as the bank's needs evolved. It determined that a cloud-based solution with robust, built-in features would provide more flexibility and give the bank more in-house control.

It turned to Bottomline Technologies to explore upgrade options to its existing fraud solution. Bottomline has been a trusted partner to the bank for more than a decade, and worked with it to scope out the fraud prevention requirements, including internal behavior monitoring needs. Ultimately the bank chose Bottomline's Insider and Employee Fraud solution to provide the expanded insider fraud monitoring the bank needed to build a more effective defense against internal threats.

As part of the Bottomline's Fraud and Financial Crime Management solution solution set, the cloud-based Insider and Employee Fraud platform employs user behavior analytics to quickly identify unusual user activity and stop harmful actions before the damage is done. The bank was particularly interested in the solution's unique ability to track all user and account activity in a non-invasive manner, which allowed business to be conducted without interruption. Other appealing features included seamless connectivity across multiple platform types (i.e. mainframe, internet, mobile) as well as screen-by-screen replay functionality and cross-channel behavioral profiling. With changing work environments and a shift to increased remote employees, the bank realized it required a more aggressive approach to stay vigilant and fight internal fraud.

The upgrade, which the bank implemented directly out-of-the-box (no customization needed) and chose to host on Amazon's cloud, **included a library of more than 100 pre-set fraud detection rules.** The fact that the solution was ready to go as is, made it a streamlined implementation process and allowed the bank to quickly strengthen its defenses against internal attacks and human error.

NEW CONFIDENCE

With the new solution in place, employee behavior is now automatically tracked and profiled through the analytics engine, powered by rules-based detection.

The solution allows the banks' investigation team to efficiently manage and document the process when investigating internal fraud alerts. The Investigation Center feature provides a consolidated view of all relevant activity including alerts, cases and user profiles.

With the new platform in place, the bank was able to enhance its protection against insider fraud and prevent future off-limit access. It plans to expand the monitoring of additional systems with the highly-scalable solution to ensure even greater protection.

The bank chose to activate **70 pre-set rules** and Bottomline's Insider and Employee Fraud now seamlessly monitors the activity of numerous employees, accessing more than **5M accounts**, across multiple applications and platforms. This activity equates to **400K internal transactions** daily, all monitored in real-time and all tracked with screen-by-screen, auditable trails.

Learn how your organization can act on internal suspicious behavior as it occurs, rather than after the damage is done.

READ NOW

EMEA Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA

Phone: 0870-081-8250
Toll-free: +44-118-982-2253
emea-info@bottomline.com