Bottomline

A Banker's Guide to Insider Fraud

6 Steps to Stay Ahead and Block the Threat

Fraud is an increasingly serious threat for businesses around the world, eroding data integrity and security, consumer confidence and brand integrity. When fraud is discussed, often hackers or external fraudsters come to mind. However, insider fraud is a critical threat that is growing. According to Aite Group, insider fraud is predicted to have a resurgence in 2020, in fact 43 percent of FIs expect that employee fraud rates will increase in 2020.[1]

In addition to the direct cost of the fraud, some organizations receive monetary fines from authorities for having inadequate controls or allowing the fraud to occur. In 2018 the median fine was $100,000 with 20% being fined for over $1 million.[2]

As shown in the chart below, personal pressures and poor market conditions can raise the incidence of internal fraud but organizational culture can reduce the trend.

MARKET TRENDS	MARKET IMPLICATIONS
Motivation or pressure can cause an employee to look for opportunities to steal; the employee may rationalize the actions by thinking it is just a loan or that they deserve the money.	Employees who are motivated to steal will do so unless there is s strong ethical culture, internal controls that are observed regularly, and deterrents in place to convince the employee the risk is not worth the potential reward.
Employee fraud tends to lessen during sound economic times and heighten when the economy worsens.	The economy has been strong in recent years, but when it slows, the rate of employee fraud incidents will rise.
Consumers are concerned over reading about inappropriate employee behaviors and want to be assured that their FI is monitoring employees' actions to protect their data and accounts.	Strong controls and an ethical environment won't just hinder employee fraud incidents but are also likely to attract and maintain good employees. Consumers will have greater trust in the FI if they know this environment exists.
Employees often fear reporting fraud or suspicious activity out of fear of reprisals.	FIs that offer confidential reporting options available to employees will reap the benefits.

Source: Aite Group

6 Steps to Locking Out Insider Fraud

1. MONITOR ALL USER BEHAVIOR

In order to detect potential insider fraud, businesses need to monitor and recognize unusual employee behavior in real-time. Suspicious behavior can be detected by using monitoring systems to track when employees perform unusual changes to information systems. Unfortunately fraud may be detected only after damages have been incurred.

A better way to prevent fraud is to monitor data searches in order to detect when employees may be planning fraud. For example, if a bank employee is attempting to deplete a dormant account, the first step is to find inactive accounts with high balances. By monitoring user queries, investigators can recognize when employees are looking for potential targets before a dormant account is re-activated or money is transferred.

2. COMPARE AN INDIVIDUAL'S BEHAVIOR WITH THE RELEVANT PEER GROUP

Employees who attempt to commit fraud are typically familiar with the controls that have been put in place and can circumvent them. For example, bank employees that know the transaction threshold can siphon off smaller amounts of money over a longer periods of time to avoid detection.

An analytics engine — one that uses intelligent machine learning to quickly identify the normal behavior of individuals and compare with other employees with similar roles — can be more accurate at identifying fraud attempts. For example, a back office employee makes a query to discover inactive accounts just before they are automatically flagged as dormant; this behavior can be flagged as suspicious when compared with typical queries conducted by peers.

3. DETECT COMMONALITIES IN EMPLOYEES' ACTIONS

Two employees conducting an excessive amount of activity on the same customer accounts can be a clear indication of collusion, especially if they are the only employees to access these accounts. For example, if a back office clerk and a bank teller are consistently viewing the same accounts, this can be an indication that they are working together to take over these accounts. One way to identify and prevent this type of collusion is through comprehensive rules-based detection which will alert fraud investigators. This in combination with intelligent machine learning and behavioral profiling can provide organizations with a comprehensive understanding of the commonalities within their employees' actions.

4. USE VISUAL TOOLS TO LINK EMPLOYEES, CUSTOMER ACCOUNTS AND SUSPICIOUS ACTIVITIES

Organizations typically segregate functions between roles to lessen the opportunities for employees to commit fraud. For example, in banks typically only back office clerks can reactivate a dormant account, but they cannot transfer funds. Tellers, on the other hand, can transfer funds, but cannot change account status. For detecting such schemes, an anti-fraud system needs to monitor and correlate all activity across back office, transactional systems, branch offices, e-channels and other systems.

Visual link analysis can be very effective in detecting suspicious events. It can uncover sophisticated scenarios that are difficult to uncover using traditional tables and charts. Using tools that can cluster events and identify trends with a visual display speeds up investigation and resolution.

By using link analysis to monitor and analyze employee activity, organizations can detect suspicious activity before any funds are lost or their reputation is tarnished. This monitoring works best when combined with an internal fraud training program and a reporting hotline for employees to report fraud. Employees are less likely to commit fraud if they know there is a greater chance of being caught.

To learn more visit us on our website or watch our video about Cyber Fraud & Risk Management

▷ WATCH NOW

5. ANALYTICS ALONE IS NOT ENOUGH – ADD TRAINING AND AWARENESS

Technical countermeasures only address part of the problem. Training and awareness are also key measures to inform employees on the proper processes. Even more importantly, it informs them that there are security measures in place which can often deter employees who may be considering committing internal fraud.

6. DON'T RELY ON AUDITS

Regular fraud and compliance audits don't mean you are safe. The Association of Certified Fraud Examiners cites that internal audits only detect fraud 15% of the time, while external audit merely 4%.

Thirteen percent of FIs admit they have not audited or reviewed employee fraud processes in the last two years, and hard to believe but 22% say they don't know if they have conducted an audit. Audits clearly have limitations as sampling may not be enough to capture the whole story, and fraudsters who are always on the move may be too clever for inexperienced auditors. Not only that, but many audits are heavily influenced by their assessment of internal controls which may or may not be adequate.

CONTACT US

1. Aite Group, Employee Fraud: Anticipate a Resurgence, January 2020.
2. Association of Certified Fraud Examiners, 2018 Report to the Nations

Bottomline

Corporate Headquarters
325 Corporate Drive
Portsmouth, NH 03801
United States of America

Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
info@bottomline.com