Fraud.net

8 Actions to Take Now to Reduce Insider Fraud

Table of Contents

Introduction: Why Focus on Insider Fraud?

> **The ACFE (Association of Certified Fraud Examiners) estimates 5% of company revenue is stolen through insider fraud. If you are a leader, whether CISO, CIO, or CFO, you need to be addressing this issue now, to bring that money back to your bottom line.**
>
> **- Whitney Anderson, CEO of Fraud.net**

Among cyber fraud and related criminal schemes, those originating from inside your organization can be the most damaging and challenging to detect and prevent.

While it requires a multi-function, top-down approach to combat insider threats, an AI-centric model is the linchpin to a proactive and sustainable **path to preventing insider fraud**.

The approach includes better utilization of something you have in abundance - organizational data in its many forms and from many functions. But data alone is not enough to deter insider fraud; you need data with context. By contextualizing the data through advanced AI, you can hone in on abnormal activity, and quickly stop insider schemes.

THE INCREASING THREAT OF INSIDER FRAUD

Cybersecurity incident data can be challenging to nail down, and insider fraud is even more challenging. But one aspect of insider fraud all experts agree on - it is on the rise. How much it is rising varies by source, and is likely under-reported due to organization's reticence in reporting.

Human nature makes it easier to accept and guard against threats or criminal behavior from outsiders, than from fellow members of your group. Likewise, cybersecurity practitioners have typically placed greater focus and resources in guarding against dangers from external sources than from their organization's personnel.

Perpetrators of insider fraud run the gamut from privileged access, super-users with the expertise and malice to carry out sophisticated fraud schemes, to the "innocent" data entry associate that unwittingly exposes company information to external criminals.

47%

Increase in insider threats since 2018

43%

Percentage of insider fraud incidents over $100M

Source: PwC's 2020 Global Economic Crime and Fraud Survey

Insider Fraud Archetypes

> **We discovered in our research that insider threats are not viewed as seriously as external threats, like a cyberattack. But when companies had an insider threat, in general, they were much more costly than external incidents. This was largely because the insider that is smart, has the skills to hide the crime, for months, for years, sometimes forever.**
> **— Dr. Larry Ponemon, Chairman and Founder of Ponemon Institute**

Below are the **three primary archetypes** of insider fraud perpetrators, but all end with the same result, money absconded from your company.

MALICIOUS INSIDER

A company employee that deliberately utilizes their internal access to fraudulently profit from their actions. They exploit organizational data and systems, and sometimes other personnel, to embezzle and defraud. The employee's motivation can include: greed, notoriety, rationalization, revenge, or simply thrill seeking.

01

NEGLIGENT INSIDER

The negligent employee unwittingly enables fraudulent activity on the part of others through their actions or lack of action. The outcome can range from being duped by phishing emails, disclosing sensitive information, or inadvertently allowing access by external fraudsters. The individuals are unaware of the damage caused by their negligence.

02

MALICIOUS STAKEHOLDER

Like the malicious insider, this individual is a vendor, contractor, or former employee with access similar to an insider. They are potentially more damaging due to a lack of loyalty to the company.

03

THE COST OF INSIDER FRAUD

The cost per insider incident is staggering; a recent Ponemon survey found the average cost of insider fraud to be **$756,760 per incident.** Below are more metrics:

$4.6M

Average annual total cost to companies from negligent insiders

$4.1M

Average annual total cost to companies from malicious insiders

20+

Number of annual incidences reported by 60% of respondents

77 days

Average length of time to contain an insider incident

Source: PwC's 2020 Global Economic Crime and Fraud Survey

"The leading companies we work with spend a considerable amount of time analyzing if they are allocating sufficient resources to insider fraud. Most companies tend to put an outsized focus on external threats. It is a natural bias, as most companies are better at assessing third-party risks, and have typically invested significantly to detect and prevent external fraud. But internal fraud is the most challenging to detect and can be the most damaging to companies."

Cathy Ross, President of Fraud.net

A New Danger - Insider Fraud-as-a-Service

The ever-expanding dark web continues to provide new opportunities for criminals to thrive. It has expanded to insider fraud, (https://www.cxotoday.com/corner-office/the-rise-of-insider-threat-as-a-service/) and created a nascent "Insider Fraud-as-a-Service". Though still small, insiders can sell information on clients, systems, financial statements, and other proprietary information on the dark web.

Some experts believe that another potentiality is for criminal enterprises to use the dark web as a recruiting hub to recruit individuals with marketable skills to be hired into targeted companies to extract valuable information.

Your organization's greater immediate risk is your privileged users, who have the access and typically the knowledge to do serious damage. This includes exfiltrating data and selling on the dark web.

Prior to the pandemic, insider threats represented an estimated 40% of all fraud losses.

COVID's Impact on Insider Fraud

COVID's transformation of the work environment has dramatically impacted the amount of insider fraud. Even with some return to normalcy in our work environment, the changes will continue to increase your organization's potential harm from insider threats.

Security team's focus - The pandemic's dramatic changes shifted their focus, creating opportunities for malicious insiders.

Processes - Were designed originally for traditional offices, not virtual environments. The changes brought on by the pandemic often undermine controls and allow for easier execution of fraudulent acts.

Access - The dramatic increase in cloud computing applications has altered access to systems and data. Despite the huge benefits of the cloud, it also comes with risks, as more access to data equals more opportunity for mischief.

Morale - While not empirically quantifiable, anecdotal evidence is that morale suffers in long-term isolation. Lowered morale often leads to higher incidences of fraud.

Anxiety - Concerns over job security can lead to retribution against employers or create the impetus to commit financial crimes to offset concerns of financial loss.

Porousness at the edge - Some remote worker's rapid digital transformation has gotten ahead of their digital security measures and knowledge, creating easier access for fraudsters to company information.

Take a Strategic Focus to Address Insider Fraud

Because of insider fraud's **unique attributes** compared to external threats, you need an approach that is not solely technology-driven. To sustain success, it takes new paradigms involving people, processes, and technology. The strategy needs to be centered on AI and better use of existing data, but it also must be more holistic, top-down driven, and focused on activities involving the customer lifecycle.

The AI-centric approach starts with the massive amount of data that your company generates, which must be better utilized to detect potential threats. Harnessing this data to spot potentially troublesome behavior by employees or other internal stakeholders, provides an effective early-warning system. With advanced AI and analytic techniques, like deep learning, **user entity behavior analytics (UEBA),** and advanced visualizations, you can gain new levels of insight into the potential behaviors that can lead to insider fraud.

UEBA helps to more quickly and effectively monitor employee activity to identify and isolate problematic behaviors. Pairing UEBA with insider incident response scenarios provides the framework for more timely and consistent action when risky behavior is recognized.

8 Steps to Reduce Insider Fraud Now

We believe it is imperative for companies to develop and deploy a comprehensive and sustainable program to address insider fraud. In taking a more strategic approach to insider fraud, there are eight items on your to-do list:

01.

Employee Onboarding Process

Addressing insider fraud starts before the employee starts with your organization. While background checks and the onboarding process are an important first step, do not get complacent that it is the #1 tool to fight insider fraud. Studies have found that well over half of insider fraud perpetrators did not have previous criminal records or insider fraud incidents. Most perpetrator's motivation for committing fraud begins as an employee.

02.

Culture, Controls, and Training

- Effectively addressing insider fraud over the long-term requires an organizational culture that embraces openness about cybersecurity, and reporting potential threats without fear of retribution.
- Transparency, accountability, and adherence to control measures must be driven from the top down. Executive actions need to be consistent with security policies and procedures, not open to exceptions when expedient.
- Cybersecurity training must be carried out on a regular cadence. Executives need to lead the way to emphasize the importance and the requirement to attend.

03.

Incident Scenarios

Insider threats require incident scenarios to provide the focus and framework for your mitigation efforts and response. Many companies establish plans for external attacks, but fail to prepare similarly for insider threats. By reviewing prior insider incidents, you can develop the scenarios for the most common and damaging threats. Prioritizing the scenarios creates the focus and countermeasures to better prepare your security team and organization.

04.

Data Orchestration

Bringing together and organizing relevant data from throughout the organization, plus external sources, is at the heart of addressing insider fraud. For example, Fraud.net's Insider Threat Data Orchestration methodology employs a variety of company, proprietary, and externally-sourced data, including:

- Employee logins, activity, and location
- Other pertinent employee information, including social media
- Vendor, customer, and other relevant internal databases
- Data from Fraud.net's identity and behavioral analysis tool
- Information on leaked credentials from our dark web credential monitoring solution
- Fraud.net's global consortium of data on known fraudulent entities
- Applicable third-party data through APIs, based on your organization's needs

05. **Customer Lifecycle-driven**

Focusing on transactions and activity in the customer lifecycle processes is an essential focal point in addressing insider fraud. Analyzing the entire lifecycle helps you identify anomalies in the process by focusing on activities involving:

- Devices
- Logins
- Applications
- Transactions
- Outcomes

You also gain insights into improving workflows and controls to prevent the recurrence of fraud.

06. **Deep Learning Models**

Because of the complexity, high-dimensionality, diversity, and dearth of insider fraud data sets, it is best analyzed using deep learning models. Along with user behavior data, and other related data that must be scrutinized, the models can learn the many levels of hidden representations in the data sets. By utilizing UEBAs to profile and risk score user behavior, your organization is better equipped to detect anomalies, and potential criminal conduct.

07. **Advanced Visualizations**

Leading technology tools are of little value without presenting the information in an easy-to-understand, actionable manner. Intuitive visualizations with risk scoring provide you with the ability to quickly scan for potential anomalies for further investigation. The aim is to reduce the number of potential cases reviewed, and false positives generated.

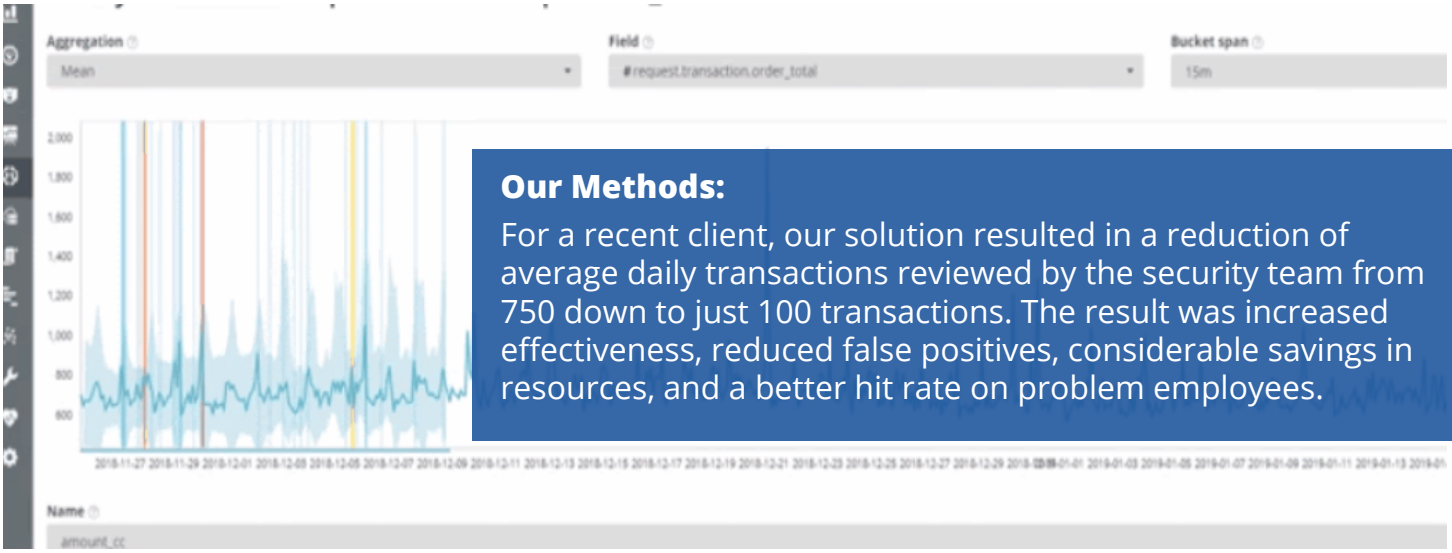
08. **Continuous Monitoring**

Lastly, and unquestionably not least, is the continual training, awareness, and monitoring required to stay ahead of insider fraud. Circling back to item #2, leading companies build a culture that ensures the controls and training put in place initially, remain embedded.

OUR RESULTS: ACHIEVING A 90% REDUCTION IN INSIDER FRAUD

Fraud.net was brought in to help address a leading online travel agency's fraud issues. Within the first week of analyzing the call center agents, 5% of agent's activities were problematic and showed signs of potential insider fraud. This discovery and subsequent removal of problem agents, led to a 10%+ reduction in the overall fraud rate. In the end, insider fraud was decreased by 90%, driven by deep learning algorithms comparing agent-level behaviors and outcomes.

While technology is not the sole answer to addressing the challenge of insider threats, advanced AI technologies can provide you with a powerful tool to combat them. Critical to creating a more resilient organization is ensuring employees are not defrauding your organization and making challenging times even tougher.



Our Methods:

For a recent client, our solution resulted in a reduction of average daily transactions reviewed by the security team from 750 down to just 100 transactions. The result was increased effectiveness, reduced false positives, considerable savings in resources, and a better hit rate on problem employees.

Partner with the Experts

The Fraud.net insider fraud solution is a lightweight data and low impact implementation for your team. We do the heavy lifting with our cloud-based solution, requiring little effort from your company. Many similar solutions only focus on agent logs, approvals, or other specific elements. We probe the whole spectrum of relevant data and potential issues enabling **insider threats**.

Our UEBA provides deep learning models, swift anomaly detection, geolocation, and behavioral analyses to promptly detect high-risk behavior by insiders. Using the Fraud.net end-to-end anti-fraud system, your organization can more effectively:

- Generate access, transaction, and account audits
- Analyze activity by operational group
- Establish prioritization, workflow, and accountability to manage findings, remediation plans, and exceptions
- Enable faster discovery and reaction times to mitigate emerging risks

Fraud.net's solution also provides sophisticated visualizations to quickly highlight potential anomalies that require further investigation. Our advanced tools help reduce false positives, giving your team more time to focus on the real problems. The result is diminished insider risk, and a more secure and resilient organization.

Learn more about why Fraud.net's platform, a cloud-based "glass-box" system, is the most advanced and intelligent option for comprehensive insider fraud prevention and detection.

LEARN MORE