DATAVISOR

6-STEP GUIDE TO BUILDING A

FRAUD AUDIT PROGRAM

The cost of fraud is staggering. According to a recent report from the Association of Certified Fraud Examiners, a single instance of fraud costs organizations an average of $1.5 million. That money comes directly out of your bottom line — money that could be better spent on marketing, technology, business upgrades, or other activities that will help you maintain a competitive edge.

That's why it's advisable for you to build fraud detection into your auditing processes. Let's look at what it takes to build a successful fraud audit program.

1 Assign Team Members to Auditing Roles

Audit procedures to detect fraud take a proactive approach. Assign people to these responsibilities so they can become in-house experts in this area. For larger enterprises, these might be standalone roles. For smaller companies, someone on your fraud detection team may take these responsibilities in addition to other work.

The bottom line is that auditing for fraud can't be left to chance. The best audit procedures to detect fraud are supported by skilled, capable personnel to detect symptoms and take their auditing to the next step.

2 Assess Your Fraud Risks

Risk assessments are common tools used in organizations of all shapes and sizes. Though these assessments are not designed to detect acts of fraud, they can reveal whether your organization has the necessary tools, people, and other resources to mitigate acts of fraud.

Writing out fraud risks into statements is a critical step in developing a fraud audit program. These risks shed light on how fraud occurs and how it can go undetected. You should also include any vulnerabilities in your internal controls that could allow fraud to thrive.

For example, you might write a fraud risk statement that goes something like this:
"Customers' accounts are being hacked and unauthorized orders are being placed with their credentials, resulting in costly chargebacks to the company."

A fraud auditor's job is to go through each fraud risk statement to identify areas for improvement in fraud detection controls. For this fraud risk statement, questions an auditor might ask include:

- How does the company verify user identities?
- Do we have two-factor authentication controls in place?
- How do we send notice when a person's account may have been compromised?
- How can we cross-reference purchase data with customer credentials (e.g., Did the order originate from the customer's IP address, physical address, etc.?)

The answers to these questions can help organizations start to tighten their controls and mitigate acts of fraud.

3 Conduct Internal Control Testing

With written risk statements, fraud auditors can start to look for signs that fraud is occurring in their organization.

Let's use the same example. When doing internal control testing, fraud auditors might look to see if orders that result in chargebacks are using the same customer credentials as valid orders.

If you find that a lot of your chargebacks are using different addresses or coming from different IP addresses compared to the same customers' valid orders, then you might need a better way to cross-reference this data before an order is processed.

Keep in mind that a symptom of fraud doesn't necessarily mean that fraud is occurring. For example, customers may place an order from a spouse's computer, which would result in a different IP address. Or, they might have a gift shipped directly to the recipient instead of their own house, which would result in a different physical address.

The goal is for internal control testing to help you win bigger and lose smaller over time. Catching more acts of fraud can significantly reduce the financial impact of fraud on your company.

4 Investigate the Symptoms

Detecting symptoms of fraud should trigger red flags that spur additional investigation. Using the above example of fraudulent orders and chargebacks, you wouldn't necessarily cancel the order without first looking into whether the order is valid.

Taking a manual approach could mean calling or emailing the customer directly and asking them about the order.

An automated approach to this step is to "test" the potential act of fraud against other criteria. For example, you might use software to cross-reference multiple data points for that customer, such as IP address, device ID, physical address, and credit card number. If all of these things are different than normal, it could make a strong case for fraud. But if only the IP address has changed, for example, then it could be the person simply used a different device to place their order.

5 Determine a Frequency for the Fraud Audit Program

Fraud is constantly evolving, which means your fraud audit program will need to evolve, too. This means starting with assessing your fraud risk statements to ensure you're hitting on all current possibilities, then moving through each process to detect instances of fraud.

6 Invest in the Right Tools to Facilitate the Fraud Audit Program

Each of the above steps to auditing fraud can be better executed with the right technology and tools. A fraud audit can be a largely manual process, which also means it can be a time-consuming one. However, modern automation tools can help you perform many of these steps in real time and at scale to help you do more with your fraud detection resources and protect your bottom line.

For example, DataVisor's open machine learning modeling platform provides full transparency to build and audit models, fully supporting model governance at every level.

DataVisor's Knowledge Graph enables fraud teams to perform link analysis by visualizing connections among various entities. Instead of manually going through data, users can instantly see connections in real time and how they compare to billions of other entities and events. This is an essential step in identifying large-scale coordinated fraud attacks and sophisticated attack patterns that may otherwise look normal on a case-by-case basis.

Further, DataVisor's case management functionality maintains a complete audit trail, recording all fraud team actions. All fraud detection results are paired with easy-to-understand reason codes, giving your fraud team access to exceptional explainability for any audit inquiries.

Final Thoughts

The right tools can help companies decrease the costs of a fraud audit program, streamline the process for faster results, and reduce false positives that can lead to high customer friction and poor user experiences.

Request a demo today.

Learn about how DataVisor can help you fight fraud.

SCHEDULE A DEMO

About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform for enterprises. Using proprietary unsupervised machine learning algorithms, DataVisor restores trust in digital commerce by enabling organizations to proactively detect and act on fast-evolving fraud patterns, and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of more than 4B global user accounts, DataVisor protects against financial and reputational damage across a variety of industries, including financial services, marketplaces, ecommerce, and social platforms.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR