



## A GUIDE TO

# How to Build an Effective Fraud Team

# Introduction

---

Effective teams are greater than the sum of their parts. Much like a well-oiled machine, teams should be intentionally designed to work together to fulfill a common mission. That is certainly the case when building a fraud team.

Although technology plays an essential role in executing the team's various functions and is interwoven in everything the team will do to fight fraud, it's the people who will be in charge of using the technology that will produce the intended outcomes. In other words, your fraud detection and prevention tools and strategies are only as good as the people deploying them and using them every day to make decisions.

Therefore, your fraud team should be composed of members who are dedicated to the cause. They should have knowledge in risk management and experience in detecting, identifying, and preventing fraud. And last but not least, they should have the ability to analyze data to make accurate decisions in critical moments.

DataVisor VP of Product Management Steve Knopf shares more insight on what it takes to build an effective fraud team in 2021 and beyond.





## The First Hire: A Policy Manager

---

Before Steve joined DataVisor, he served as the first trust and safety hire for a popular online marketplace – one that had no established systems or policies to guide them.

“We were addressing fraud as we went and didn’t really have any policies or guidelines to follow,” he reveals. “When you don’t have a dedicated fraud team, you’re usually shooting in the dark when it comes to detecting fraud. So there’s a lot to figure out, and there’s a lot of room for error.”

Steve believes that fraud teams benefit from fraud policies to guide them so they can better determine what’s fraud, what’s not, and also what presents unacceptable risk to the company. These policies not only detail the types of fraud that occur and their early warning signs, but also how teams will be tasked with responding.

That’s why the first hire is usually a Policy Manager. This role develops and fleshes out the fraud policies that the rest of the team will rely on in detecting and responding to fraud. These policies may include:

- ▶ What customers have to do to sell or buy with a company
- ▶ Verification processes
- ▶ Setting transaction limits (gross number or dollar value)
- ▶ How the customer experience or customer care team enforces the fraud policies

The Policy Manager isn't necessarily the one who decides on policy, but they are the ones tasked with researching and collecting feedback to propose a policy that gets signed off by managers of various cross-functional departments.

Steve also notes that because new issues can arise and each company has unique nuances to consider, this position is usually a permanent position within the company.

“A lot of people try to bring in a contractor or consultant to handle fraud policy creation, but this is far from being a one-time thing. New needs arise all the time, and it’s best to have someone who knows your company well and can respond and adapt to changes over time.”





## The Next Hire: Trust and Safety Detection Analyst

---

The Trust and Safety Detection Analyst works with the selected technologies to detect and automate responses to suspected fraud and risk. Oftentimes a rules engine is and should be employed. Rules are written based on behaviors the analyst detects, and these rules are constantly rewritten based on changes in behavior.

Knowing the types of fraud your business may face can help to guide your selection process for tools and technology to support the fraud rules, and ultimately the people who will use them.

“Most companies have a mix of in-house-built technology, third-party technology, and business intelligence. These tools use automation to help you make sense of what’s going on with your platform or website (or other channels) so you can respond quickly and appropriately.”

According to Steve, automation combines heavily with policies.

“When you get a fraud notification, you may want to use human judgment to determine whether it’s fraud. But in some cases, fraud will be very obvious, and these are the ones you don’t need people to look at. Action in these instances can be automatically taken. So aligning policies with your automated fraud workflows is essential in saving time and capturing larger amounts of fraud.”

DataVisor is a trusted partner for this stage of the process. Our solutions help to establish processes regarding rules engines and automation much faster and with greater accuracy than companies could do from scratch. DataVisor can also detect acts of fraud that would evade human review by looking at clusters of behaviors rather than single activities. In addition to its rules engine capabilities, DataVisor utilizes a multi-pronged fraud detection approach which includes supervised machine learning, unsupervised machine learning, device intelligence, linkage analysis, and a global intelligence network to provide comprehensive, real-time fraud detection.



## Next Steps: Enrich Your Customer Care Team

---

Steve mentions that most organizations already have a customer care team in place before they consider building a fraud team. The Customer Care Team members are usually the ones helping users log into their account, answering questions, and ensuring a frictionless customer experience. But while these requests might not seem fraudulent in nature, they could be opportunities to commit fraud.

That's why Steve recommends extending fraud-related knowledge to employees who directly interface with customers.

“Start loading up the team with a checklist of how to detect fraud or showing them ways users can commit fraud through customer service activities. This level of cooperation can be extremely critical to your business, plus it helps you scale your fraud detection efforts as you grow.”

If adding to the responsibilities of the customer care team is not an option, Steve says that building a separate trust and safety team is a solid equivalent. “You need people who can review items that come across as fraudulent and make decisions where automation isn't always sufficient. Tools like DataVisor provide a good balance here because DataVisor automatically logs why an activity is suspicious and creates visuals around those reasons, so trust and safety teams can make faster decisions.”



## Filling in the Gaps

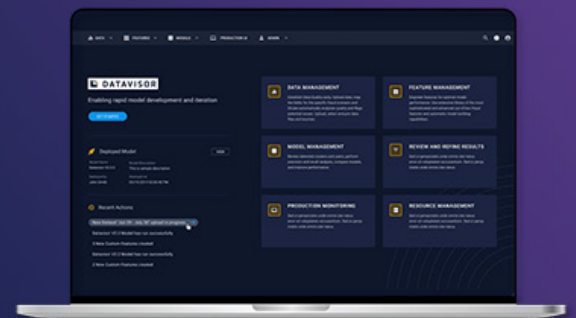
By this point, Steve says that the key pieces of your fraud team are in place. The rest of the team should be built based on scaling the business and the business model of the company. Other common positions you may want to fill at this point include rules analysts, business intelligence team members, and trust and safety operations team members, depending on your unique business needs. Then, it's a matter of filling in any gaps with technology, such as business intelligence, to ensure the fraud team is delivering value.

See how DataVisor supports effective fraud teams. [Get a demo and experience proactive AI-powered fraud prevention today.](#)

# Experience proactive AI-powered fraud prevention today.

GET A DEMO

 DATAVISOR



### Insight from 4.2 Billion+ Users and 800 Billion+ Events



Financial Services



E-Commerce



Social Platform



Mobile & Gaming



Telecom & Travel



Insurance

### CONTACT US

If you are interested in learning how DataVisor can help bring your fraud detection to the next level or wish to start a trial to assess your current fraud exposure level, please contact us at: [info@datavisor.com](mailto:info@datavisor.com) or visit us at [www.datavisor.com](http://www.datavisor.com)

### DATAVISOR

967 N. Shoreline Blvd.  
Mountain View | CA 94043