Mindset and Measurement:
The Keys to Attacking Your False-Positive Problem

CNP CARD NOT PRESENT®
NEWS, EDUCATION AND EVENTS
DECODING DIGITAL PAYMENTS & FRAUD

sift

“No.”

It’s a tough word to hear. Especially for online consumers. They searched for an item, found exactly what they wanted on your site, entered their card number, and then? Denied. Their credit is good and they’ve always paid their bills on time. Confusion gives way to frustration and perhaps even anger. Why? You’ve unjustly accused them of being a fraudster—you’ve insulted them.

The anger your insult caused usually doesn’t last long, though—just long enough for them to navigate over to your competitor’s site and successfully make their purchase. If you’re lucky, you lost just that sale. But it’s likely you’ve permanently lost a customer.

Merchants that sell online, and the technology they use, are becoming better and better at spotting fraud. But, if a fraud department puts too much emphasis on limiting loss from fraud, rather than maximizing the number of legitimate transactions it approves, merchants could be rejecting more orders than they should be.

In a recent study, more than a third of consumers (36 percent) said they had tried to make an online purchase but were falsely declined *(Sift, January 2020)*. For younger consumers, the rate was even higher: Fifty-six percent of shoppers in the highly valued 25-35 year old demographic had been declined due to suspected fraud. And, the study found, a significant percentage of consumers (25 percent) who experienced these declines—these insults—did take their business elsewhere.

So, how should merchants engaged in this dilemma—dealing with the natural tension between preventing fraud and negatively impacting a convenient, frictionless user experience—move forward? Commit to thinking differently about the false-positive problem itself and to effectively measuring your false-positive rate.

> *“If you think about the issue as insulting your customers—you’re accusing them of taking suspicious actions when they’re actually doing nothing wrong—it creates a more emotional response within the company.”*

Getting Your Mind Right

The term “false-positive” was born in laboratories—it’s used often in medicine. It simply means when the result of a test shows something is present when it really isn’t. And, while it’s perfectly accurate in the scenario where a fraud system flags a legitimate transaction as suspicious, it’s clinical and impersonal.

According to Kevin Lee, Trust & Safety Architect at Sift, the phrase doesn’t really account for the effect it has on a visitor to your site. Instead of trying to figure what their false-positive rate is, at Sift they call it “customer insult rate.”

“The reason we use the word ‘insult,’ and it’s a term I’ve been using for at least seven years, is because we wanted to elicit a more visceral, emotional response on the part of our team, whereas ‘false-positive’ is mathematical, maybe colder,” Lee explains. “If you think about the issue as insulting your customers—you’re accusing them of taking suspicious actions when they’re actually doing nothing wrong—it creates a more emotional response within the company.”

Percentage of e-commerce merchants unaware of what their false positive rate is

40%

30%

Percentage of e-commerce merchants who don’t even attempt to measure their false politive rate

It’s just one way the company tries to use philosophy and mindset to change what they do and how they are perceived.

Another is embracing a shift that many newer, forward-thinking merchants engaged in the digital economy are also championing—transitioning from a “fraud department” to a corporate structure that includes a “trust and safety department.” It implies a focus on establishing trust with customers and prioritizing their experience rather than simply preventing fraud loss.

Organizations with a trust and safety philosophy understand the effect false-positives—customer insults—have on a customer's lifetime value and the balance required to include user experience in the calculation that is made while rooting out fraud.

"The shift to a trust and safety mindset is table stakes now," Lee says. "The most advanced companies we work with, whether they are tech-focused like Airbnb or non-tech like American Apparel, have moved to this model. And, customer insults are hugely important to the businesses that function this way because everything is about user experience."

The Internet has made access to goods and services ubiquitous, according to Lee, so user experience becomes the most important way companies distinguish themselves. Being able to connect their work within the company to UX is vital and evolving to a trust and safety mindset is one way down that path.

"If they don't, they'll continue to be shut out of important decision-making within their company," he said. "The growth teams and the product teams are just going to launch things and the risk teams are just going to have to clean up whatever mess happens."

The State of Measurement

More important than what you call the phenomenon or your team, however, is having an accurate picture of exactly how many false-positives your current fraud prevention system yields. Only then can you see the true nature of the problem and the effect it is having on your revenue.

Measuring false-positives, though, is a significant challenge. So much so, that a surprising number of companies ignore the problem completely—despite the short-term lost sale and, potentially, the long-term lost customer. Not only are more than 40 percent of e-commerce merchants unaware of what their false-positive rate is, but 30 percent say they don't even attempt to measure it *(2018 Fraud Operations Study, Card Not Present).*

> *"…companies are relying more on automation. And, if you're not checking the quality of those automations, you could be in trouble."*

It's hard, as the adage goes, to prove a negative. But, that's what you're trying to quantify—the absence of fraud—and that's why many companies throw up their hands. But, there are ways to attack the problem.

A recent study found there were a number of ways companies attempt to track false-positives. Forty percent said they look at calls or emails from customers who complain about getting declined, 36 percent track the rate of approvals when customers retry their transaction after being declined, and 31 percent review declined transactions after the fact to try to determine which might have been legitimate *(2018 Fraud Operations Study, Card Not Present).*

All these actions can give you some insight into your false-positive rate. But, according to Lee, these tactics will consistently underreport your true number of false-positives because they are based on customers who take time to contact you or who try to make their purchase again. Lee says the best way is to follow a procedure developed by his team at a former employer.

"We created various holdout groups," he explains. "You have a scenario where our fraud system would have declined a certain number of orders for some reason. But, for the sake of learning, we would tag them appropriately and let them go. If chargebacks or abuse come back on those transactions, we know our system correctly identified fraud in that scenario. If zero chargebacks come through, you know you're insulting 100 percent of the people you think are fraudsters."

Lee stresses that a company's model or vertical are important to consider when deciding how many false-positives are tolerable in your situation compared to how aggressive you want to be in identifying fraud.

"If you're a company that has super-high margins selling digital goods and you're not hitting up against any chargeback monitoring programs, you may want to insult nearly zero customers. But if you're selling luxury goods, where one instance of fraud can be very expensive, maybe you do want to be a bit more careful."

Of course, not every company has the manpower and expertise available to access their data and conduct such experiments. But, companies that have the resources can use this analysis to their benefit.

> *"...recognizing what is fraud and what is a customer insult is even more challenging than usual because consumer behavior has shifted"*

Customer Insult and Covid-19

While global stay-at-home orders in March and April 2020 caused online traffic for some e-commerce verticals to spike (e.g., streaming video services, online grocery and many retail segments), overall e-commerce traffic is down, according to Sift's analysis of transactions on its network. At the same time, fraud rates are rising. In this environment, the challenging problem of recognizing what is fraud and what is a customer insult is even more challenging than usual because consumer behavior has shifted.

"Let's say I used to order two rolls of toilet paper at a time," Lee explains. "Now, because there are shortages, if I can order 10 rolls at a time, that's what I do. It's still me, but the velocity or the volume I'm purchasing in now is changing. If the store I'm buying from is using an anti-fraud system that is not able to respond quickly enough to my change in behavior, it might decline my transaction, even though I'm a legitimate buyer. Right now, every good order you have is even more precious."

We are in a situation right now where there are fewer transactions overall and user behavior has become more erratic. At the same time, fraud departments that used to rely on manual reviews may not have access to those workers anymore—they might be furloughed or even laid off. "As a result," Lee says, "companies are relying more on automation. And, if you're not checking the quality of those automations, you could be in trouble."

> *"...if you're selling luxury goods, where one instance of fraud can be very expensive, maybe you do want to be a bit more careful"*

Insult Monitor

One thing fraud departments have been largely unable to automate themselves is the process of effectively measuring false-positives. Part of the reason is a lack of resources. Many e-commerce merchants lack the engineers and data scientists needed to implement the kind of experiments Lee noted above that can accurately determine a false-positive rate.

To that end, Sift has added a functionality to its automation platform that enables customers without the technical resources to run those experiments by choosing a few simple parameters and letting it run. Users have the flexibility to run multiple experiments in different scenarios, stop and start experiments as they choose, or change parameters at any time. Experiments run for 30 days and will accurately calculate your false-positive rate and provide insights that can be used to reduce false-positives.

It arms fraud professionals with a very powerful metric to tell their story within companies, which don't often understand or value what they do. Often, bad reviews on social media or stories of declines that get back to corporate executives can further damage fraud or trust and safety teams' standing. Significantly reducing the false-positive rate can add revenue in a demonstrable way and empower risk teams to enhance their standing with data—not be the victim of anecdotes.

Percentage of consumers who tried to make an online purchase and were falsely declined **36%**

56% Percentage of shoppers in the highly valued 25-35 year old demographic who have been declined due to suspected fraud

Percentage of consumers who experienced these declines that took their business elsewhere **25%**

ABOUT SIFT

Sift is the leader in Digital Trust & Safety. Powered by the most sophisticated, real-time machine learning technology and a global community of fraud fighters, we combine custom models with learnings from across our global network of 34,000 sites to identify trusted users and fraudsters with unparalleled accuracy. Sift detects evolving fraud patterns automatically—enabling you to reduce losses and build trust with customers without the need to scale manual review efforts as user and transaction volumes grow.
Learn more at at Sift.com.

ABOUT CARD NOT PRESENT®

Card Not Present, part of the RELX Group, is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. For more information, visit CardNotPresent.com.

© Copyright 2020 Card Not Present®

This document was produced as a joint effort between Card Not Present® and Sift.

CNP CARD NOT PRESENT®
NEWS, EDUCATION AND EVENTS
DECODING DIGITAL PAYMENTS & FRAUD

sift