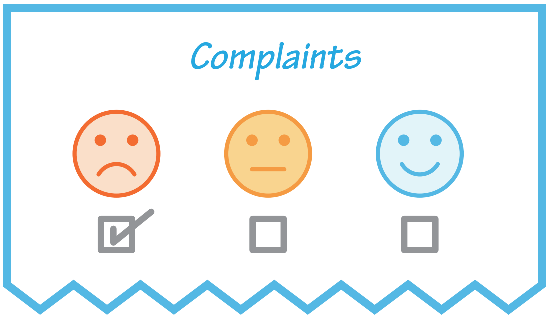
KICKSTART

YOUR FRAUD-FIGHTING STRATEGY

Meet Ankit

Got Fraud? Ankit does. And he's starting to get nervous.

You see, Ankit is a product manager at SingleRoom, an up-and-coming vacation booking site aimed at single travelers. SingleRoom has it all: brilliant technical team, wise investors, a roadmap for growth. But recently, some customers have started reporting a troubling complaint...They're being conned into paying for rooms that don't exist. Camouflaged between all the swank Tokyo studios and quaint rooms in Tuscan farmhouses are fake listings sporting misleading stock photos. Once an unsuspecting vacationer contacts the lister, they're directed to pay through a different website. Sound fishy? It 100% is. And this growing fraud problem is irking legitimate customers, who've started telling their friends that SingleRoom is a scammy site.



Meet Ankit

SingleRoom is also growing its user base (yay!), which means it's processing more credit card orders (double yay!). But the finance team has started complaining about the growing pain of credit card chargebacks, those niggling fees assessed when a business lets fraudulent transactions through the door. They were asking – no, begging – for a solution that would block these orders before they went through.

"BUT I DON'T WANT TO GET IN THE WAY OF GOOD CUSTOMERS! Everyone says SingleRoom is fast and easy to use – reserve with a single click. The last thing I want is to mess that up."

Sound familiar? Fraud cuts across industries and geographies, affecting companies of all sizes. If you're reading this book, you're probably dealing with some kind of shady behavior on your site – whether it's fake transactions or fake accounts.

We're here to give you some practical tips for recognizing, understanding, and fighting fraud and account abuse.

And we have a special guide for you and Ankit...

Meet Siftie

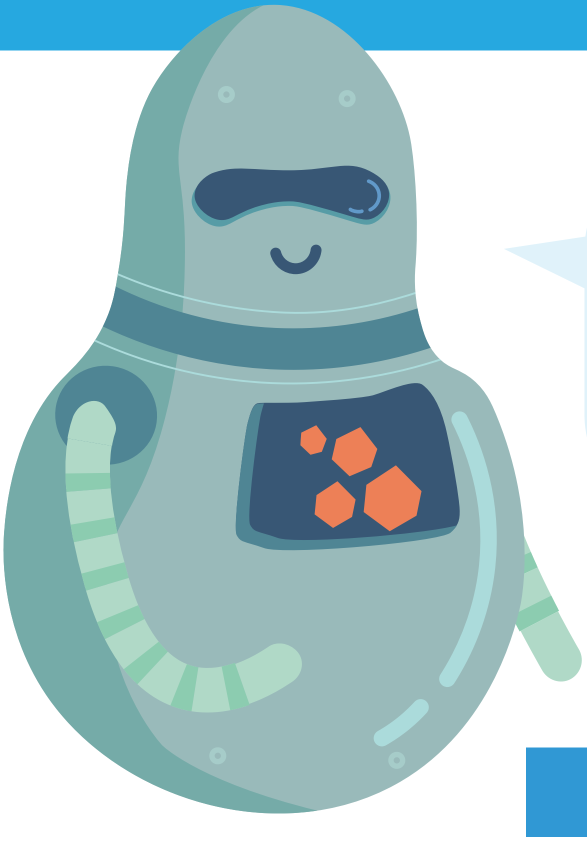
You’re in luck!

Siftie has a taken a rare break from his role as project manager, inspirational speaker, and mindfulness guru for all of Sift Science’s machines to give you and Ankit the background on:

01

FRAUD IN THE WILD

Payments Fraud & Account Abuse

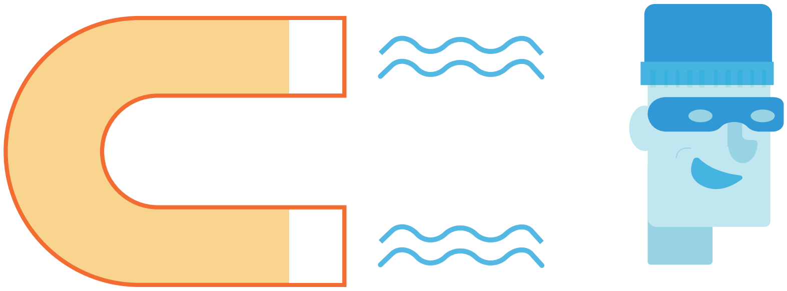


The world of fraud is vast and imposing, but we're going to focus on two common types of bad online behavior: **payments fraud** and **account abuse.**

	PAYMENTS FRAUD	ACCOUNT ABUSE
WHAT THE BAD GUY DOES	Uses stolen or counterfeit payment information	Opens fake account or uses their real account to scam or spam
COMMON EXAMPLES	• Fraudulent orders • Credit card testing • Gift card fraud	• Online scams • Phishing • Referral code abuse
HOW IT HURTS YOUR BOTTOM LINE	• Chargeback fees • Refunds • Replacement orders	Money lost to fake "users"
HOW IT HURTS YOUR TOP LINE	Lost sales from incorrectly blocked customers	Lost users due to poor experience

What Makes a Business a Fraud Target?

Reducing friction and encouraging quick transactions are ways to appeal to customers, but they may also inadvertently open your site up to malicious users.



Here are 5 magnets that draw fraudsters:

Real-time fulfillment

Whether it's delivering shoes or groceries, fraudsters capitalize on the short window for reviewing orders.

Digital cash

Gift cards, virtual currencies, and money transfers are all delivered instantly – without the need for a shipping address.

Referral programs and coupon codes

These programs offer a low barrier for fraudsters.

Easy sign-up

Removing friction for legitimate customers also removes hurdles for fraudsters who want to exploit your site and your users.

Users exchanging goods or services

Marketplaces can face both account abuse (the lister) and transactional fraud (often, the buyer). Fraud can come from either side...or both.

That's what I'm dealing with! Can you give me the TL;DR about chargebacks?

Chargebacks: The Crib Notes

"Here's a basic overview. If you're interested, you can read tons more at All About Chargebacks."

1. It all starts with a customer telling their bank that they shouldn't have been billed for something.
2. Sometimes the customer's not being truthful or forgot they bought something (so-called "friendly fraud"), but other times their credit card number was stolen.
3. Customers have up to 6 months to complain, so chargebacks typically hit merchants about 2 to 3 months after the purchase.
4. You can dispute chargebacks. However, merchants win only 40% of those disputes.
5. If you're levied with a chargeback, the bank retrieves the money from your account plus a fee.
6. Getting a large number of chargebacks? Visa and Mastercard could fine you, jack up your fees, and even (eventually) revoke your account. Bad news.

The True Cost of Payments Fraud

“Psst...it’s not just $$$. There are hidden costs you may not be thinking about.”

Direct Cost	Opportunity Cost	Brand Cost
The cost of the product (if you’re selling physical merchandise)	Too many charge-backs? You might be barred from accepting a certain type of card	Customers may doubt the security of your site
Chargeback fees (typically $5-$20)	Time spent dealing with chargebacks = time NOT spent growing your business	Customers may complain to friends and family, and on social media
Money spent hiring people to deal with chargebacks	Accidentally turn away a good customer? There’s a lost sale	Your brand’s reputation may suffer, and you can lose potential sales

Read more about the impact of fraud

Types of Account Abuse

So, what do we mean by “account abuse”?

We’re talking about all flavors of malicious and annoying behavior that come with fake accounts on your site, or when users use their legitimate accounts for non-legitimate reasons.

FAKE ACCOUNTS

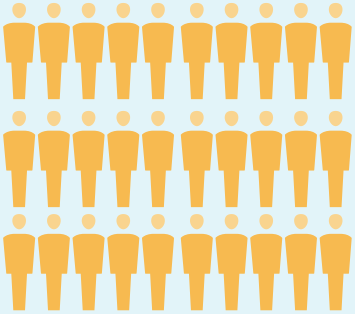
TROLLS

SPAMMERS

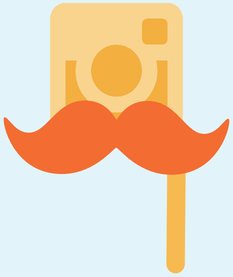
SCAMMERS

BOTS

140MM Facebook accounts are fake



8% of Instagram accounts are fake



Consumers lost $781 million to Internet scams in 2013

How Account Abuse Damages Your Brand

User experience suffers

The classic adage "one bad apple spoils the bunch" definitely applies when you've got people creating accounts and posting content on your site. Just a single bad experience could sour someone on using your service.

You have a responsibility to protect your good users from harm, harassment, and abuse on your site. If you're putting user experience high on your priority list (and you should), tackling fake accounts should be part of your game plan.

Your users start checking out your competitors

When scammers and spammers abuse your site, it's your brand that takes the heat as users take their business elsewhere.

A user who's scammed or harassed can share their opinions with their friends, family, and the public on social media.

A fraud-free site is a competitive advantage, so it makes sense to invest in preventing bad behavior up front.

No time to grow your business when you're policing spammers

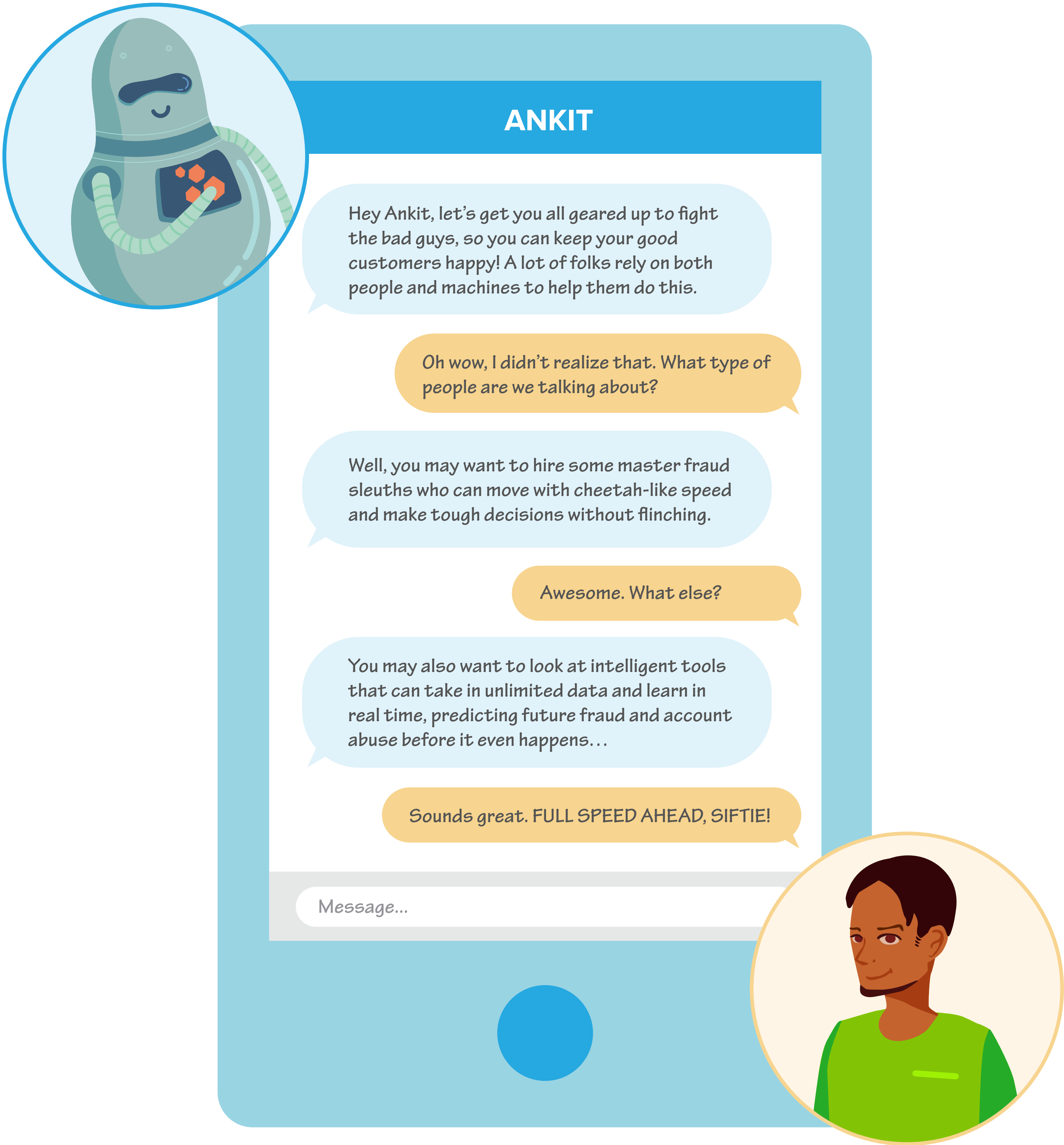
What may at first seem like a manageable problem that you and your team can handle with manual reviews and community flagging may grow into a black hole of moderating, policing, and poring over data to try and sort the good users from the bad. Sound like a great use of your time? We didn't think so.

Good question!
But first, let's take a look at how to craft your fraud approach.

02

CRAFTING YOUR FRAUD APPROACH

Getting Equipped to Fight Fraud



ANKIT

Hey Ankit, let's get you all geared up to fight the bad guys, so you can keep your good customers happy! A lot of folks rely on both people and machines to help them do this.

Oh wow, I didn't realize that. What type of people are we talking about?

Well, you may want to hire some master fraud sleuths who can move with cheetah-like speed and make tough decisions without flinching.

Awesome. What else?

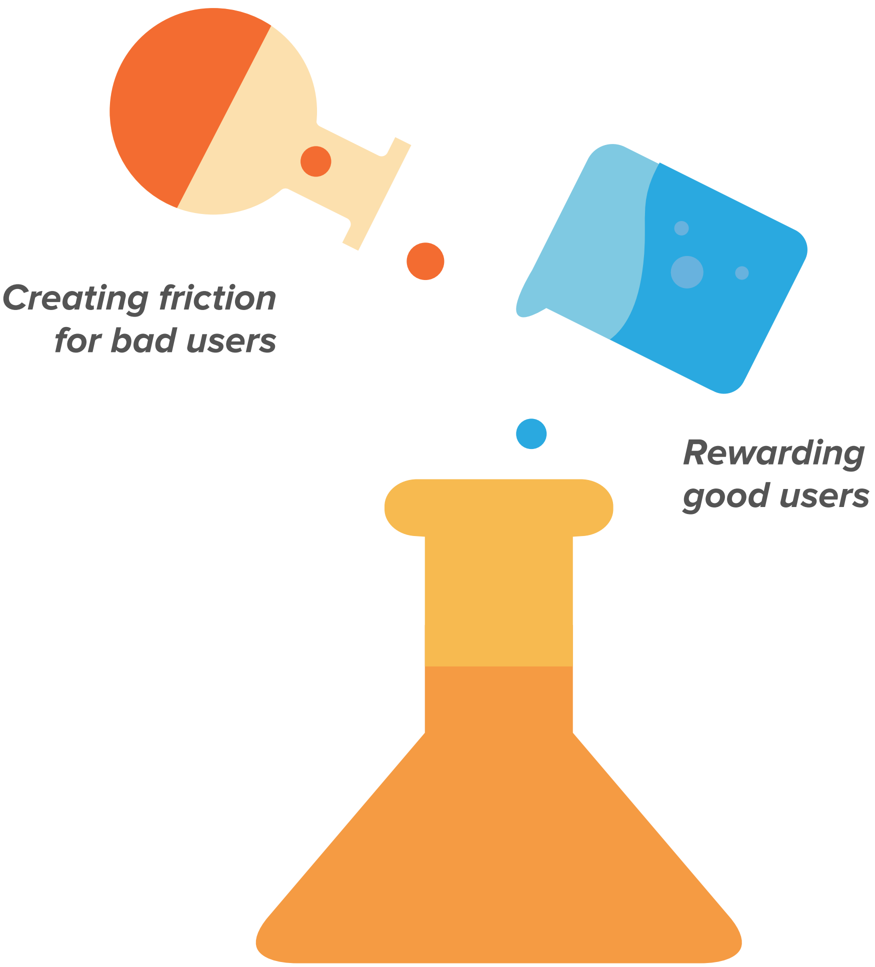
You may also want to look at intelligent tools that can take in unlimited data and learn in real time, predicting future fraud and account abuse before it even happens…

Sounds great. FULL SPEED AHEAD, SIFTIE!

Friction: A Delicate Balance

The trade-off

As you craft your fraud-fighting approach, there's a trade-off you should always keep in mind. You'll find yourself tweaking this formula until you get it right.



The more friction you create, the more likely you are to block some good customers along the way. But if you let down too many barriers, you open yourself up to fraudsters – who prey on sites with few roadblocks.

Making Customers Happy

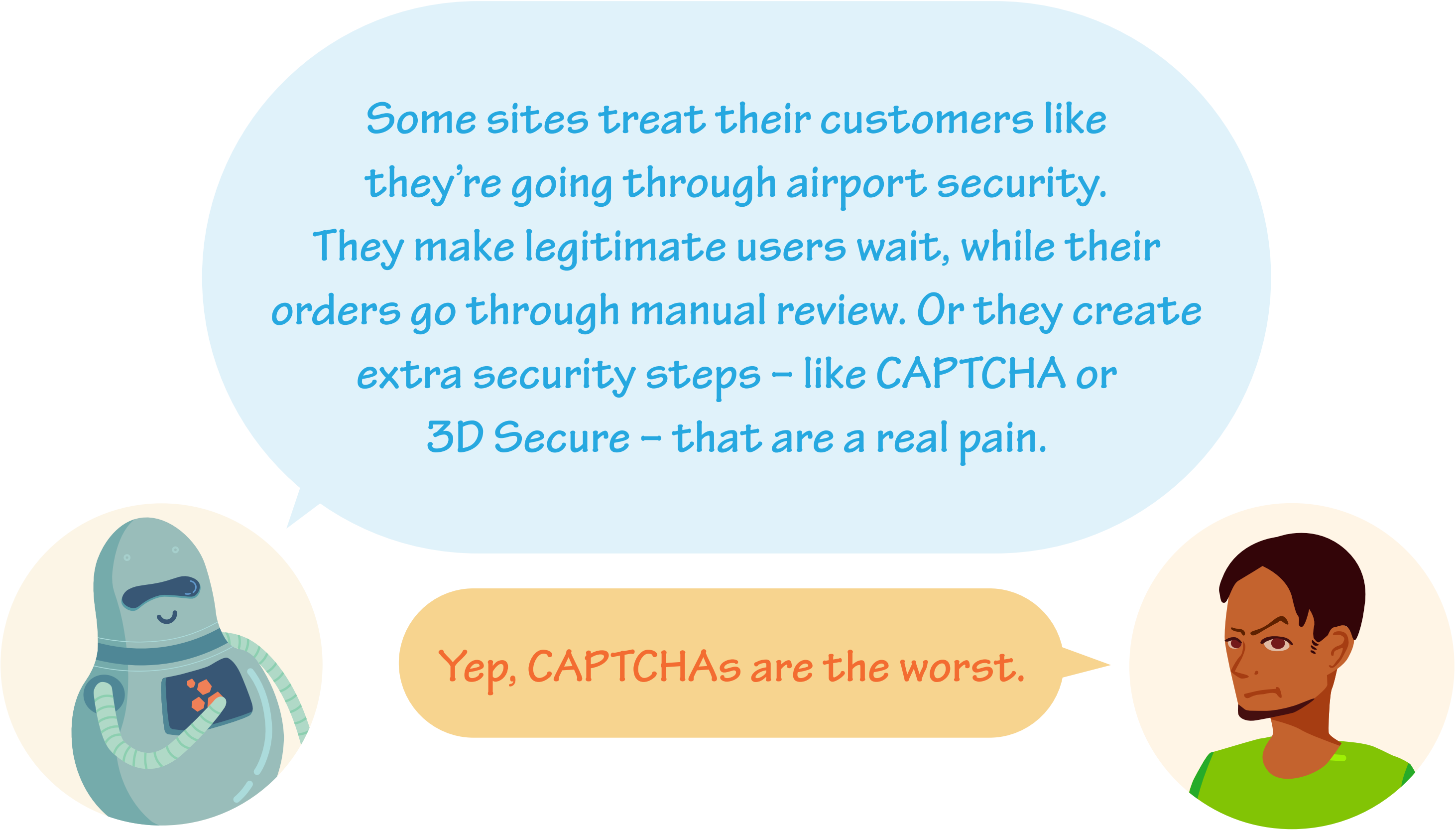
Smart fraud prevention isn’t just about keeping bad users out.

It’s about increasing conversions.

When you know who your low-risk users are, you can make it as easy as possible for them to fly through checkout, filling in fewer form fields, avoiding 3D Secure and other roadblocks that lead to drop-off.

It’s about improving the user experience.

People love – no, they adore – sites and apps that are fast and easy to use. Just look at the wild success of Amazon one-click ordering. The popularity of Uber. The brand loyalty afforded to Zappos, who made returns a piece of cake.


Some sites treat their customers like they’re going through airport security. They make legitimate users wait, while their orders go through manual review. Or they create extra security steps – like CAPTCHA or 3D Secure – that are a real pain.
Yep, CAPTCHAs are the worst.

Making Customers Happy

Two sides of the coin

In some companies, the fraud folks and the sales and marketing folks may feel at odds. After all, they have different aims, right?

TRADITIONAL GOALS AND DESIRES

FRAUD TEAM		MARKETING TEAM
Mitigating risk		Optimizing conversion
Preventing loss	VS	Growing top-line revenue
Conservative approach to approvals		Wants as many conversions as possible

When starting and growing your fraud team, make sure they're not siloed. Ideally, everyone – product, marketing, UX – should be discussing the organization's shared goals, and making sure they're working together to achieve them.

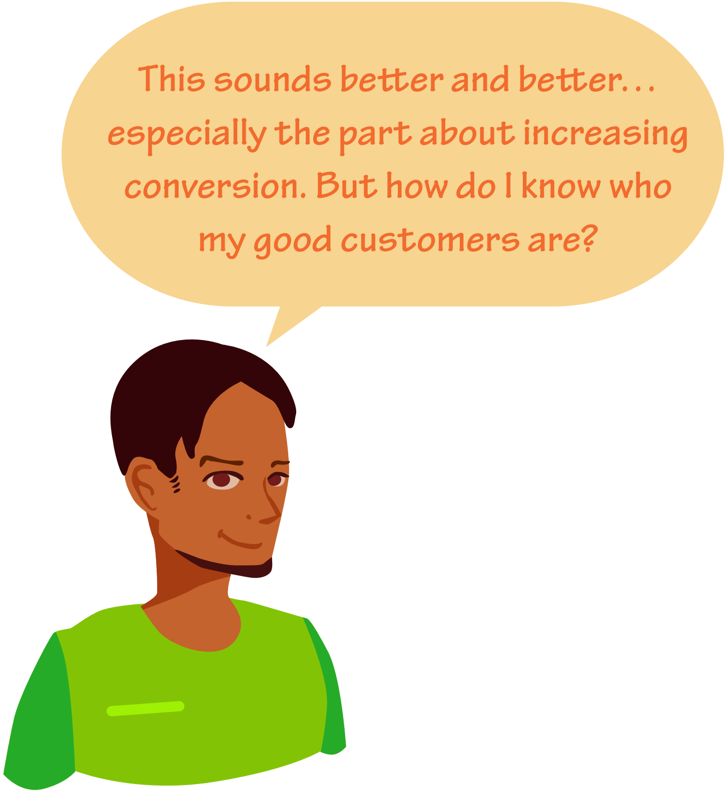
3 ideas for working smarter together

Increasing conversion

If you know which users are low-risk, UX design can create a tailored checkout flow for them with fewer form fields.

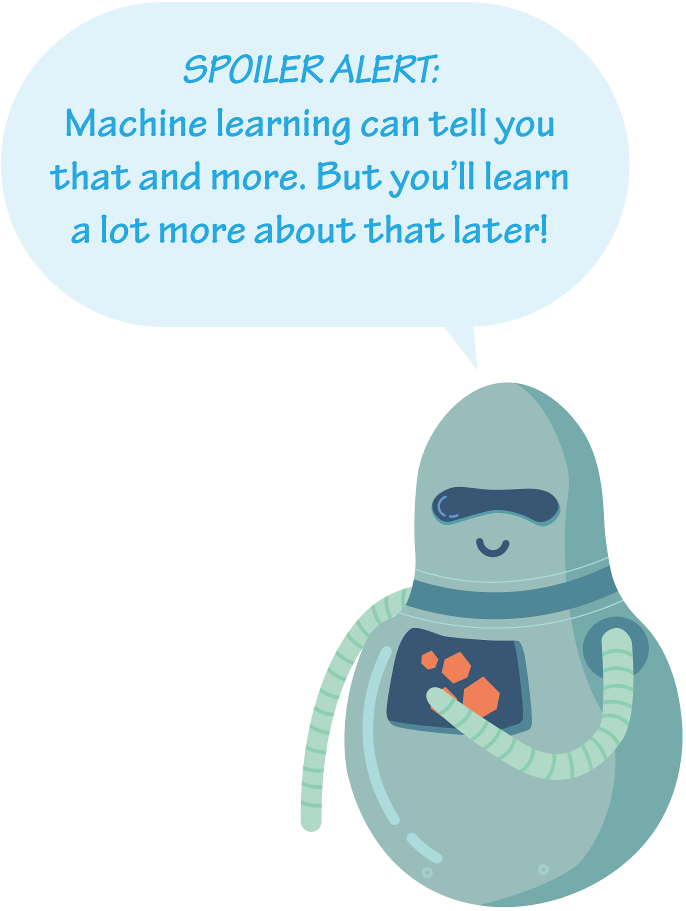
Reducing false positives

Noticed that a large chunk of legitimate users who click “buy” aren’t making it through? Tackling false positives together can help determine whether any recent website changes may have caused this spike.


This sounds better and better… especially the part about increasing conversion. But how do I know who my good customers are?

Boosting brand sentiment

Seeing complaints on social media from users whose orders were delayed for manual review – or falsely rejected? When marketing and fraud teams join forces, you can adjust your approach and improve brand perception.


SPOILER ALERT:
Machine learning can tell you that and more. But you’ll learn a lot more about that later!

Questions to Consider

“The answers to these questions will help you craft a fraud-fighting approach that’s right for your company.”

How much risk are you comfortable with?

Remember, it’s a delicate balance between creating friction for bad users (which could keep some good ones out) and reducing friction for good users (which could let some bad ones in).

How much of a risk is fraud to your business?

In other words, if fraudsters were to go nuts tomorrow and take advantage of your website, how much damage could they do?

What do you want your customers to experience?

Introducing hurdles could lower fraud, but legitimate users may get fed up and start looking at your competitors.

How much fraud are you experiencing?

If you’ve got a small fraud problem, maybe an existing team – like Customer Support – could take on this responsibility. If your fraud problem is growing rapidly, you may want to consider an in-house fraud team, plus a machine learning-based fraud solution to be more efficient.

How rapidly do you need to react to fraud?

Businesses that rely on speed – like travel companies, on-demand services, and those selling digital goods – are wise to look at machine learning-based fraud solutions that learn and adapt in real time, making split-second decisions.

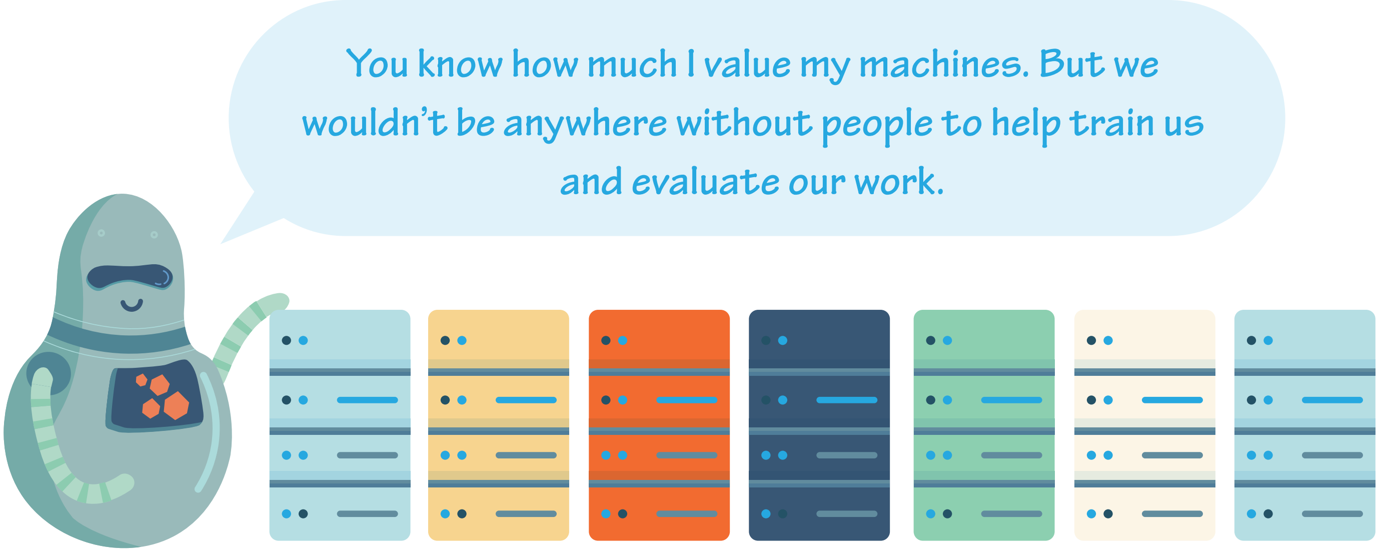
When will you be making decisions?

Is it after the payment’s been collected, after you ship a package, after you’ve issues a gift card, or at some other time? The answer to this question will help you choose the right vendor for your needs.

03

BUILDING YOUR FRAUD TEAM

What Is Manual Review?


You know how much I value my machines. But we wouldn't be anywhere without people to help train us and evaluate our work.

Finding the story

Even the best-designed fraud-detection solution will occasionally flag legitimate orders as suspicious and overlook the occasional fraudulent order. That's where people come in.

Fraud analysts manually review transactions to determine if they're legitimate or not. Essentially, they're looking for the story behind the user. An effective fraud prevention solution can automate much of this work, so analysts are only focused on reviewing a small number of orders that are truly risky.

A useful tool should also integrate with your team's workflow and makes it easy for them to verify information. For example, does the tool give an explanation for why an order's been flagged as suspicious? Is it possible to verify key data within the tool itself?

Manual review basics

When to reject held orders

What Does a Fraud Analyst Do?

A fraud analyst's job responsibilities range from the strategic to the tactical.

Analysis

Translating data into patterns and finding the gray areas in what may at first seem black and white.

Decision-making

Reviewing individual cases. For example, deciding whether an order should be approved or rejected.

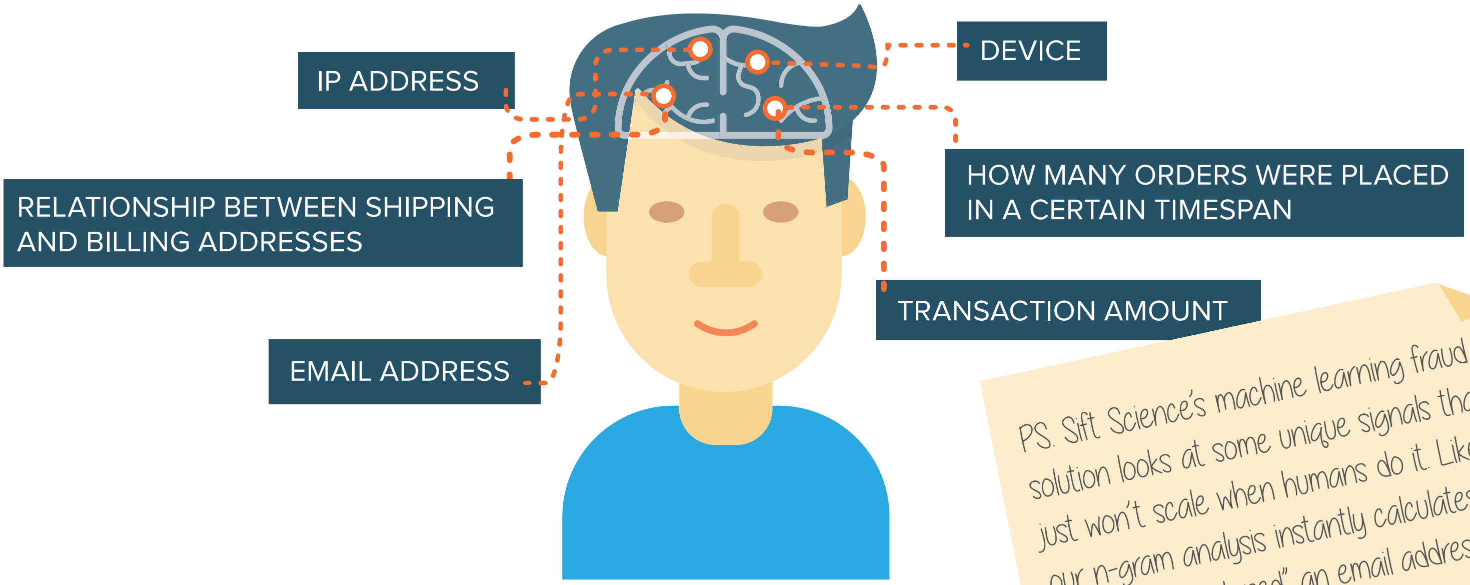
Operations

Fighting chargebacks if you have them, managing the operational load with automation, building out policies.

Communications

Following up with suspicious users as necessary for extra verification, communicating with internal teams (like Sales and Finance) about fraud-related issues.

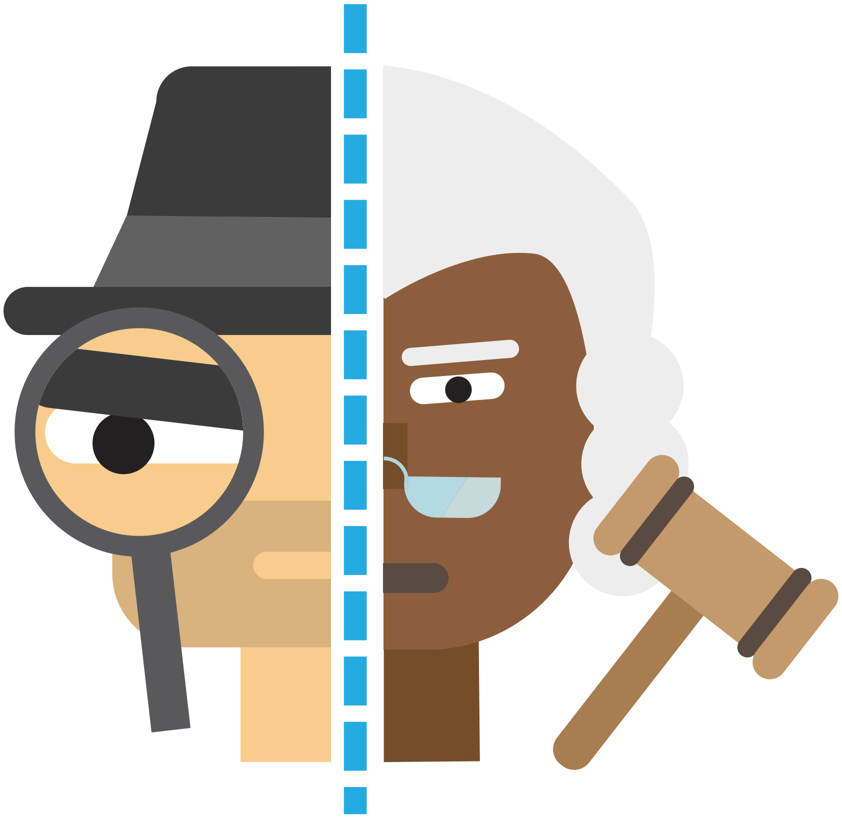
Common fraud indicators analysts look at:


IP ADDRESS
DEVICE
RELATIONSHIP BETWEEN SHIPPING AND BILLING ADDRESSES
HOW MANY ORDERS WERE PLACED IN A CERTAIN TIMESPAN
TRANSACTION AMOUNT
EMAIL ADDRESS

PS. Sift Science's machine learning fraud solution looks at some unique signals that just won't scale when humans do it. Like our n-gram analysis instantly calculates how "randomly typed" an email address is to see how risky it is.

Typical Background of a Fraud Analyst

There's no "typical" background for this role. There's no major, no college that specializes in fraud or risk analysis. Instead, focus on hiring people from different backgrounds who share qualities that will help them be successful.



PART DETECTIVE

Curious

Resists assumptions

Good at problem solving

Quick to see patterns

PART JUDGE

Takes initiative

Makes and owns decisions

Clearly explains rationale

Calm under pressure

Honing Your Fraud Team

Even though analysts don't need explicit fraud knowledge, if you don't have a lot of experience in this field it might be a good idea to hire (or at least consult with) someone who knows a bit about fraudsters, their tactics, and trends.

1. Balance two metrics: speed and accuracy

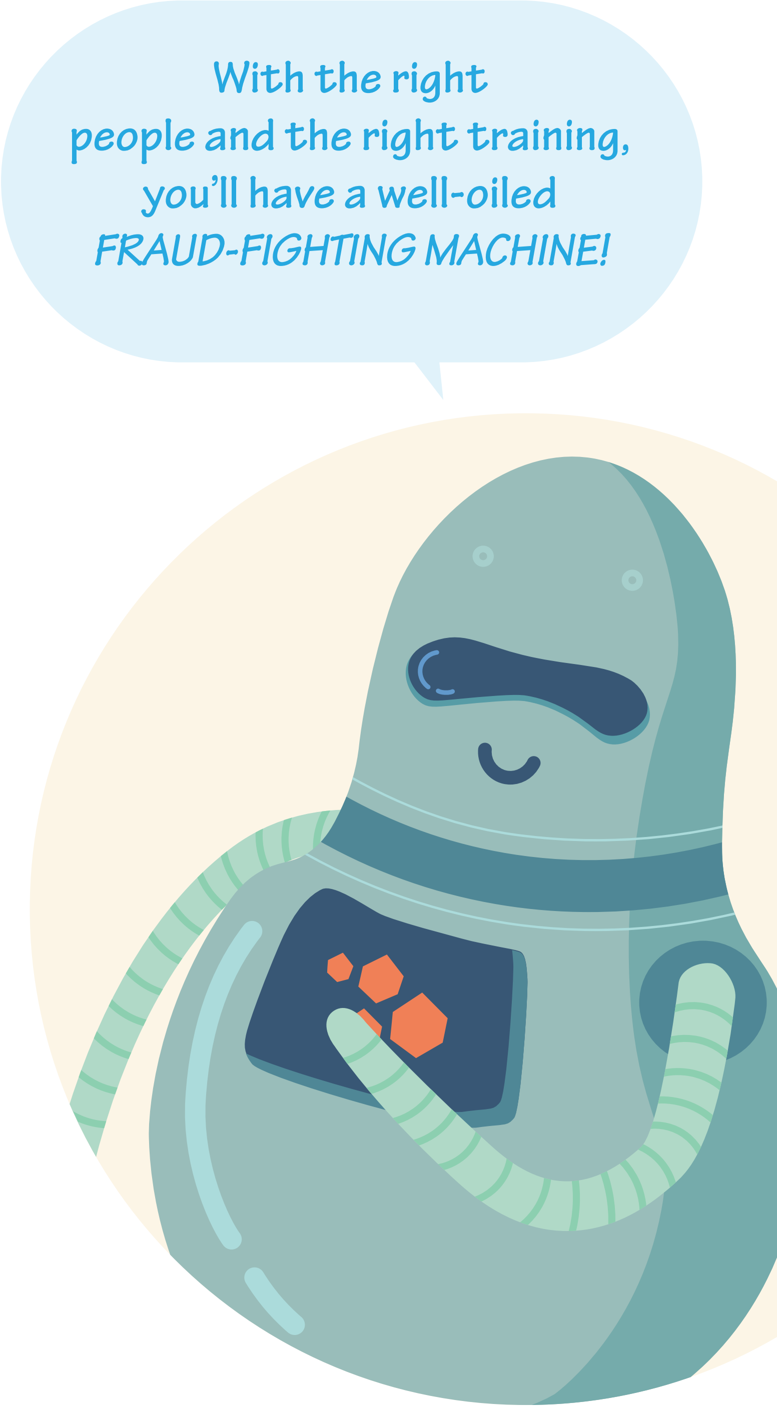
Keep in mind that faster decisions mean looking at less information. As a benchmark for speed, a typical analyst reviews 10-20 orders per hour.

2. Give regular feedback

To measure accuracy, you can audit each person's manually reviewed orders for a week. Using a sample of 20 cancelled and 20 accepted orders, check to see if the reviewer used good reasoning for each case, and give them feedback.

3. Create a source of truth

You'll never regret creating a basic how-to manual for the team so everyone's on the same page. Include criteria for canceling an order, follow-up steps after reviewing an order, and common gray areas.


With the right people and the right training, you'll have a well-oiled *FRAUD-FIGHTING MACHINE!*

04

CHOOSING A FRAUD-FIGHTING TOOL

Making Fraud-Fighting More Efficient

In the beginning, you or your fraud team might start by manually reviewing all orders and new accounts to see which are legitimate. But this level of manual review doesn’t scale. So, you may consider introducing some automation...

Rules-based system

To automate some of the common decisions you’re making, you can create “if x, then y” rules to automatically accept, block, or review transactions. For example, if you’ve noticed that transactions made between midnight and 4 am tend to be fraudier, you could have a rule to review all orders placed at 3 am where the shipping and billing address are different.

Weighted rules

However, you have to invest time in curating rules, and it can be hard to determine the overall benefit each individual rule is contributing. To mitigate the problem of black-and-white rules, you can assign each rule a point value, positive or negative, which is added together. Then, set thresholds to accept orders below, say, 500 points,reject orders above 1000 points, and review any that fall in between.

I get the rules thing. Mostly. But I’m also seeing some gray areas. Couldn’t rules end up accidentally blocking a good customer?

The Trouble with Rules

"Yep. We call that a "false positive." You make an excellent point about rules. They can be rigid, and when you have too many of them together, it can be really complex to tweak."

Imagine this scenario

- You set up could have a rule to block all reservations placed between midnight and 3am where the shipping and billing address are different.
- A college student books a room for a solo trip to Europe after a late-night study session. She's using a credit card that still lists her parents' address for billing.
- The rules flag her as a fraudster.
- You've effectively blocked that perfectly good reservation, losing perfectly good money. And frustrated a perfectly good customer.

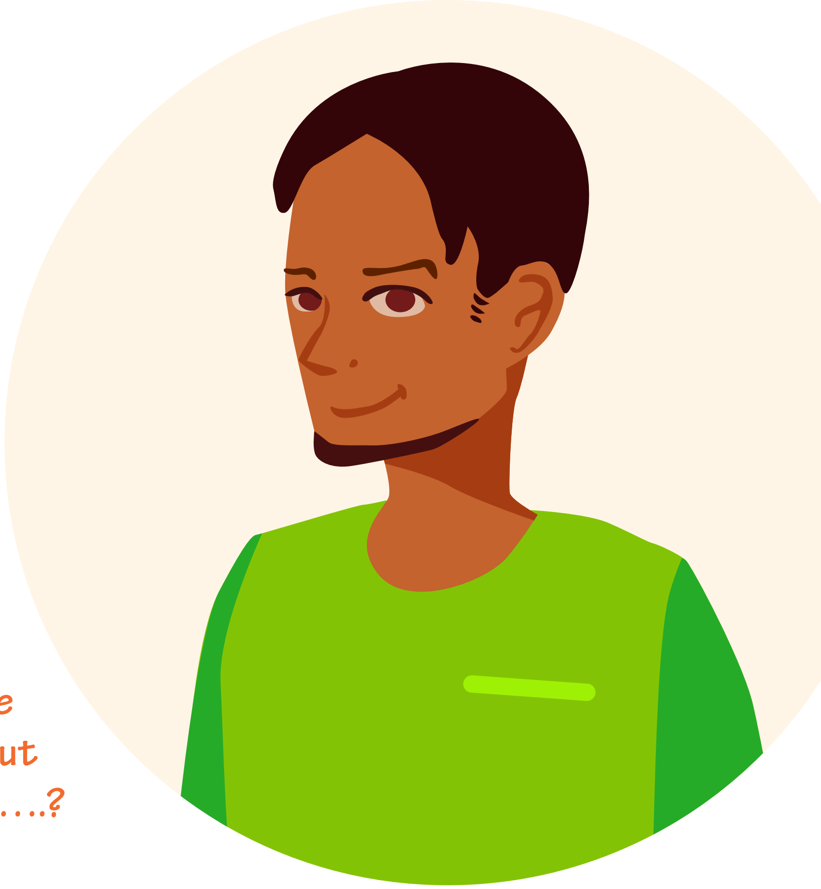
*"This is exactly what I don't want to do.
We definitely want a fraud approach that can handle nuances."*

How Machine Learning Can Help

"This is where my machines really shine! When the magic happens. Our super-smart predictive power."

Machine learning is more than a buzzword; it's transforming everything from education to healthcare. Data on its own can only tell you about what happened in the past. With machine learning, computers use specially created algorithms and mathematical formulas to learn from historical data with the goal of predicting likely future scenarios. Think of machine learning as the equivalent of a human learning from experience.

So, what's the upside for humans? Machine learning enables people to make smarter decisions faster – and with more confidence. The time it takes humans to read, synthesize, categorize, and evaluate data is significant — and machine learning streamlines much of that effort.



Yeah, I feel grateful for machine learning spam filters every time I notice my inbox is 100% free of Viagra offers. But what can it do for my fraud problem....?

Sift Science: Machine Learning in Action

Fraudsters are relentless.

They just keep coming, which can make it hard to keep up with humans alone. With Sift Science, you get a custom machine learning model that gets smarter the more data you send it.

Fraudsters are fast.

Sift Science's machine learning models learn in real time, making super-super-super quick decisions (we're talking 1 second) about whether to accept, block, or review an order.

Fraudsters adapt quickly.

Sift Science leverages a global network of thousands of fraud signals which grows stronger with every customer. The moment someone flags a user as bad, your model updates to instantly block that user.

Fraudsters are organized.

With Sift Science, you can visualize the hidden connections between different users, spotting complex fraud rings. That means you can block all of the bad guys before they even hit your site.

Shopping for a Solution

Of course, Sift Science isn't the only fraud detection software out there. After you know your needs, here are some factors to consider...

Accuracy

How accurate is the model at predicting bad actors? What are current customers saying about their results?

Tip: Testimonials and case studies can give substance to marketing claims.

Coverage

How robust is the global customer network? What industries and markets does it cover?

Tip: The more customers who are sending data, the more signals there are to learn from.

Speed

How fast does the model learn?
Do risk scores update in real time?

Tip: Sift Science updates a user's' risk scores within 1 second, based on their activity on other sites in the Sift Science global network.

Price

Is the pricing model transparent? Do you require insurance?

Tip: Solutions that offer insurance come at a premium.

Integration & Customizability

How easy is it to integrate? Can you tailor the model to your unique business needs?

Tip: It's a great idea to get your developers involved in this discussion.

Self-service & Support

Are you empowered to make changes yourself? How easy is it to get documentation?

Tip: Some solutions require you to go through them to add users and update rules.

Building a Business Case

OK, I'm ready to start talking to our exec team about fraud solutions. But I know the CFO is going to have some questions…

To be honest, quantifying the costs and benefits of fraud prevention can be tricky. Here's a start...

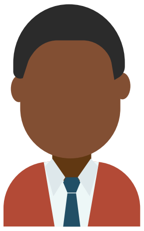
An effective third-party solution reduces your costs

- Fewer person-hours needed for manual review
- Reduction in chargeback fees, shipping, and other costs lost to fraudulent orders
- No need for your developers to update in-house rules or your fraud team to update third party rules

It also adds some costs

Fees and pricing models vary, but can include per-transaction or flat-rate monthly costs, contracts, setup fees, % of revenue, maintenance/support costs, and implementation costs.

Questions to Anticipate



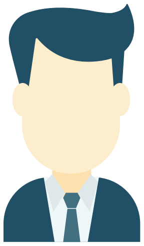
From the CTO

“What does the API documentation look like and how long will it take?”

The answers will help with resource allocation.

“Why should we devote the time to integrate now?”

An in-house tool will save developer time that might otherwise be spent updating fraud rules manually.



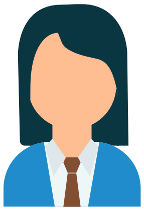
From the Fraud Manager

“How will this change our day-to-day operations?”

Is there a review console? Will it be used on its own, or in conjunction with other tools? Is there training available?

“How do I add and remove analysts, change passwords, and do any other administrative tasks?”

Some solutions empower users to do these tasks themselves, while others require you to go through an administrator.



From the CFO

“Are there any commitments involved?”

While some solutions require contracts, others are more flexible with month-to-month or per-transaction pricing.

“What’s the risk of trying a third party?”

A low-risk solution may offer a free trial, so you can see and assess results before you buy.

Customer Story: EatStreet

EATSTREET

EatStreet is an online food-ordering platform that empowers restaurants to easily accept orders via web, mobile, or social media.

CHALLENGE

When EatStreet expanded into new markets in 2014, fraud followed along. Some criminals were using stolen credit card information to place orders, and others were gaming the site's rewards program by using coupons and then canceling orders.

The on-demand nature of EatStreet's business model – people expect their food to arrive within 30-60 minutes – meant that there was very little time to manually review orders. Employee Ashley Fueger, who spent part of her day analyzing new orders, began searching for a real-time automated fraud solution.

SOLUTION

After using Sift Science's simple, straightforward API documentation to get up and running, the machine learning platform quickly began stopping fraudsters, leading to a 70% reduction in chargeback rate after the first month (and 85% the month after).

EatStreet used Sift Science to streamline their fraud workflow, auto-banning users and leveraging insights from the console to make smart decisions. As a result, they haven't had to scale up a fraud department – and other employees' time is freed up to focus on growing EatStreet's business.

Customer Story: EatStreet

EATSTREET

"Using Sift Science allows us to not waste resources on fraud. Instead, we can focus on building the best product possible for our diners."

– Ian Lavey, Director of Operations at EatStreet

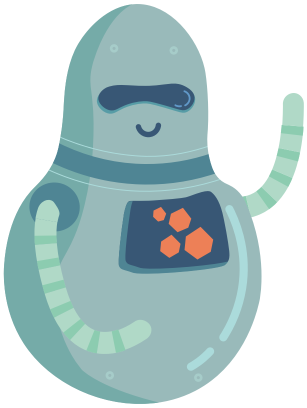
Results

★★★★★

85% **Reduction in Chargeback Rates**	**8-9x** **Return on Investment**

EatStreet uses **Sift Science** as a one-stop shop for order review, allowing them to work smarter and automate key actions.

So Long for Now!



On that note, It's time to get back to my machines…I've really enjoyed showing you the ropes, and I hope you've learned a lot.

HAPPY FRAUD FIGHTING, EVERYONE!

Cool, I've stopped sweating. Now I know how SingleRoom can kick this fraud problem.

Time to get back to business…

KEEP EXPLORING

How Sift Science works

Intro to Machine Learning ebook

How Fraud Prevention Affects Conversion white paper

Sift Science customer stories

CONTACT US

scientists@siftscience.com

www.siftscience.com