sift

Machine Learning

The Future of Fraud Fighting in the Travel Industry

Contents

Introduction: Machine learning powers trust in the travel industry

A 20-something frequent globehopper arrives in Italy, pulls out her phone, and searches for a place to stay. Visiting her favorite booking site, she instantly sees suggestions for places within walking distance, tailored to her budget. Even though she's browsing from a new country and booking at the last minute — classic signals of fraud — she's able to secure a deal for later that night and book it with a single click.

This isn't a vision of the future of travel. The technology to enable easy, personalized, and safe bookings is already here. As more and more travelers research, arrange, and buy all aspects of their trips using a digital device, the onus is on travel companies to innovatively deliver these standout experiences.

Trust vs. risk

However, if you're a travel company that sells online, you've undoubtedly encountered the flip side of enabling convenient and engaging features like last-minute bookings and streamlined checkout. Fraud and abuse threaten to run rampant.

That's why it's imperative for businesses to know which users they can trust, and which they can't. If you mistakenly allow a bad actor to buy something, create a fake account, or compromise a good user's account, the repercussions to your business can be devastating. But if you're able to instantly recognize your trusted customers, you can deliver the best experience possible — ultimately deriving more revenue and strengthening long-term customer loyalty.

The bottom line: the travel industry is evolving, and market-leading companies must invest in digital trust to stay ahead, attract new customers, and retain existing customers. And what is the technology that powers digital trust? Machine learning.

In the coming pages, we'll look at some of the common challenges faced by travel businesses when fighting fraud — and how machine learning can overcome them.

Digital opportunities

Digital bookings will exceed **$189 billion in 2017**, with mobile bookings rising to **$108 billion by 2021**.

Source: eMarketer

Digitization in travel and tourism will create **$305 billion** additional profit, plus migrate **$100 billion** of value from traditional players to new competitors.

Source: World Economic Forum

The global opportunities are vast. More than **60%** of travel bookings worldwide are still made offline, but this proportion is shrinking in all markets.

Source: Phocuswright

Fraud hits hard

Payment fraud costs the airline industry **$858 million annually**.

Source: IATA

40% of travel firms say payment fraud is their biggest challenge to deal with.

Source: Phocuswright

As much as **1-2%** of travel agency revenue is used to manage fraud.

Source: Phocuswright

Fighting fraud in travel: Top Challenges

Let's look at some of the obstacles faced by modern travel companies that are dealing with fraud and abuse.

Rising competition, small margins

The overall volume is increasing across different travel products, but many companies are facing a small margin — particularly in the airline and OTA sectors. High ticket value, with a low margin, creates a higher business risk. And "inventory" — which could have gone to a legitimate traveler — can't be recovered once it's lost to fraud.

Moving into new markets

The incredible rise of online travel has introduced great opportunities for businesses to expand into new markets. However, every new market has a different risk profile. Travel companies need to adapt their tools, as well as potentially hire new people with specialized knowledge of these markets.

Increasing product offerings

Travel companies are under pressure to grow and expand. Just look at Expedia's 2015 acquisition of Homeaway, which many say is now helping Expedia close in on Airbnb in the home-sharing market. You may start out offering a single product, like hotels. But then you expand into vacation rentals, insurance, activities, airport transportation, etc. Each product will also have a unique risk profile, which needs to be accounted for in any fraud prevention models.

Collecting information while keeping it simple

For many travel products — like airline tickets — you need to collect a lot of information. However, thanks to Amazon and other digital pioneers, customers are growing more accustomed to a streamlined buying experience. If they face too much friction, they'll turn to one of your competitors instead. How do you keep the experience simple and intuitive, without increasing risk?

Monitoring mobile bookings

Some 40% of digital travel sales are expected to be completed on mobile in 2017, according to stats from eMarketer. And Google research found that 31% of leisure travelers and 53% of business travelers have booked travel on a smartphone. Companies have to be prepared for both legitimate and fraudulent mobile bookings headed their way. When it comes to fighting fraud, mobile data is fairly unique — you can get extra data points like mobile carrier, device type, and the pressure someone uses to tap that help pinpoint fraud.

Last-minute travel is growing

The window of time between booking and traveling is shrinking for all travelers. One-third of millennials make travel plans at the last minute, and 72% of mobile hotel bookings are made within one day of a stay. This change in traveler behavior means real-time decisions are critical to your ability to stay competitive. In many cases, there's just no time to manually review risky orders and logins. Meanwhile, fraudsters take advantage of last-minute bookings to evade detection. Our research found that day-of hotel reservations are 4.3 times more likely to be fraudulent.

Flexible bookings / changing travel plans

Customer experience is high on travel companies' list of priorities — and that means providing flexibility and convenience. However, fraudsters often take advantage of the ability to change their booking at the last minute. For example, they may buy a ticket that appears low-risk ahead of time, then change it at the last minute. Not all travel companies rescreen for fraud when a booking changes.

Multiple types of fraud

Not only do travel companies deal with payment fraud in the form of stolen credit cards, but they also face fake accounts, content abuse (if they incorporate reviews and other user-generated content), and account takeover (loyalty fraud). The teams responsible for managing these different types of abuse may be located in different departments, using disparate tools, which makes it challenging to take a unified approach to managing risk.

Spotlight: How fraudsters defraud OTAs

A 2017 study conducted by Sift and Spanish OTA Destinia found trends among online booking fraud.

Fraudulent bookings:

- **Often involve third parties.** Fraudsters can pose as travel agencies to scam travelers.
- **Are high-ticket items.** The average transaction price of a fraudulent travel booking is between $283-588, so a fraudster's payoff for a faulty transaction is lucrative.
- **Are intangible.** Bookings don't need to be picked up, or re-sold like a physical item.
- **Are perishable and happen fast!** Travel bookings lose their value as soon as the date of the booking passes, so a fraudster is often in the clear once they cash out or use the fraudulent ticket or room. The time between a fraudulent transaction and the expiration can be as little as a few hours, so companies are racing against the clock to detect and block a bad purchase.

Top signals of travel fraud

- Tickets bought close to the departure date
- Tickets that are changed close to the departure time
- Tickets with multiple stopovers, but other legs of the journey are canceled
- Multiple travelers connected to a single card

Tactics used by travel fraudsters

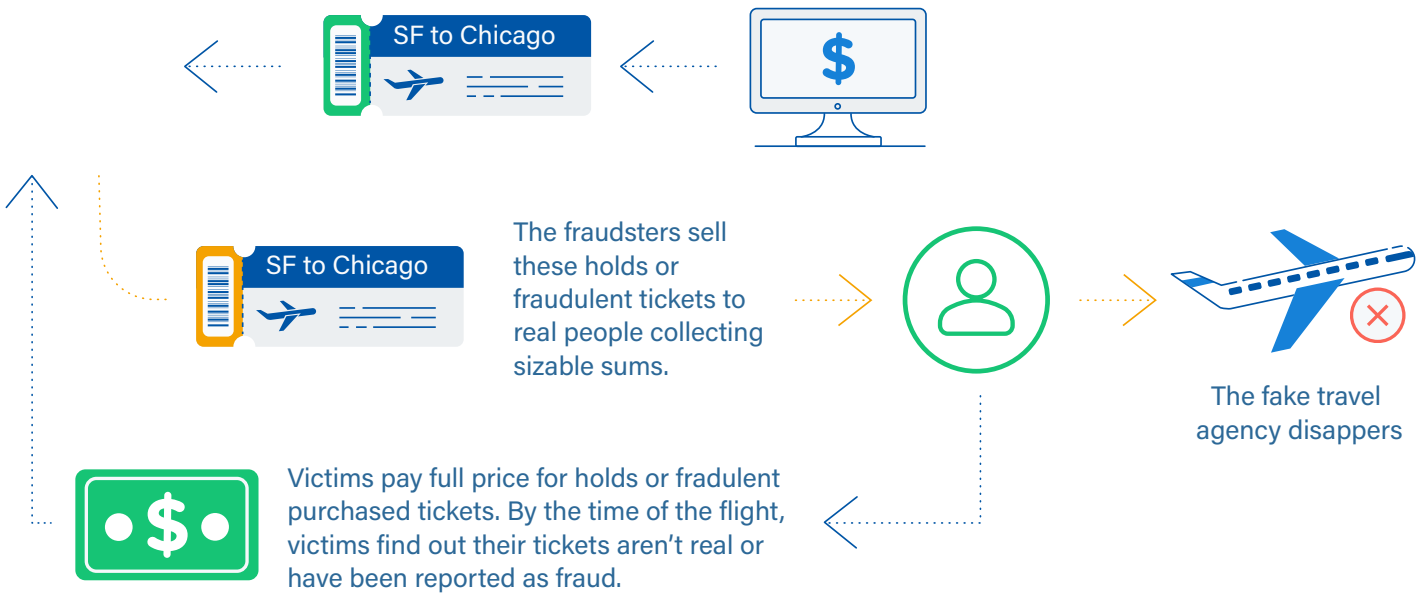
- IP masking
- Fake email addresses
- Account takeover

Taken individually, each of these actions may be normal behavior for a particular user. It's only when you apply behavioral analysis on a large scale, looking at all of a user's activity and all activity of users across the travel industry, that you can get an accurate picture of whether someone is truly who they say they are. Looking at one data point is just not deep enough.

Typical travel schemes

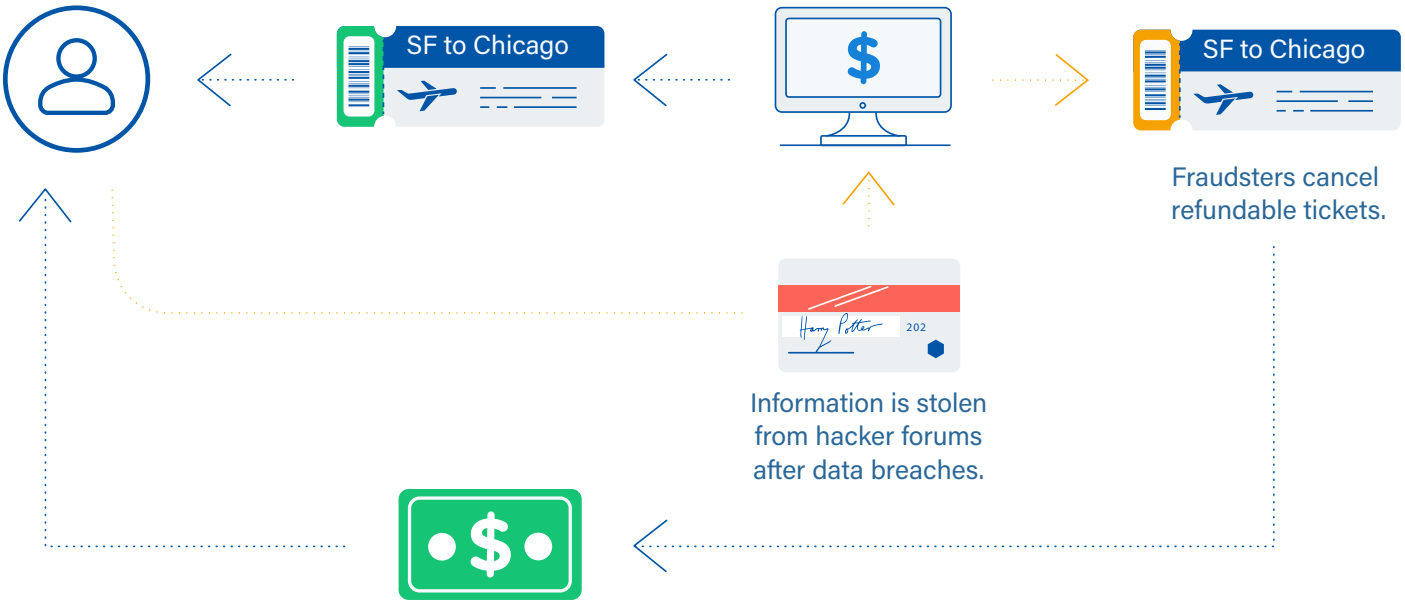
Fake travel agents

Fraudsters purchase last-minute, refundable airline tickets, train tickets or hotel rooms using stolen credit card information.



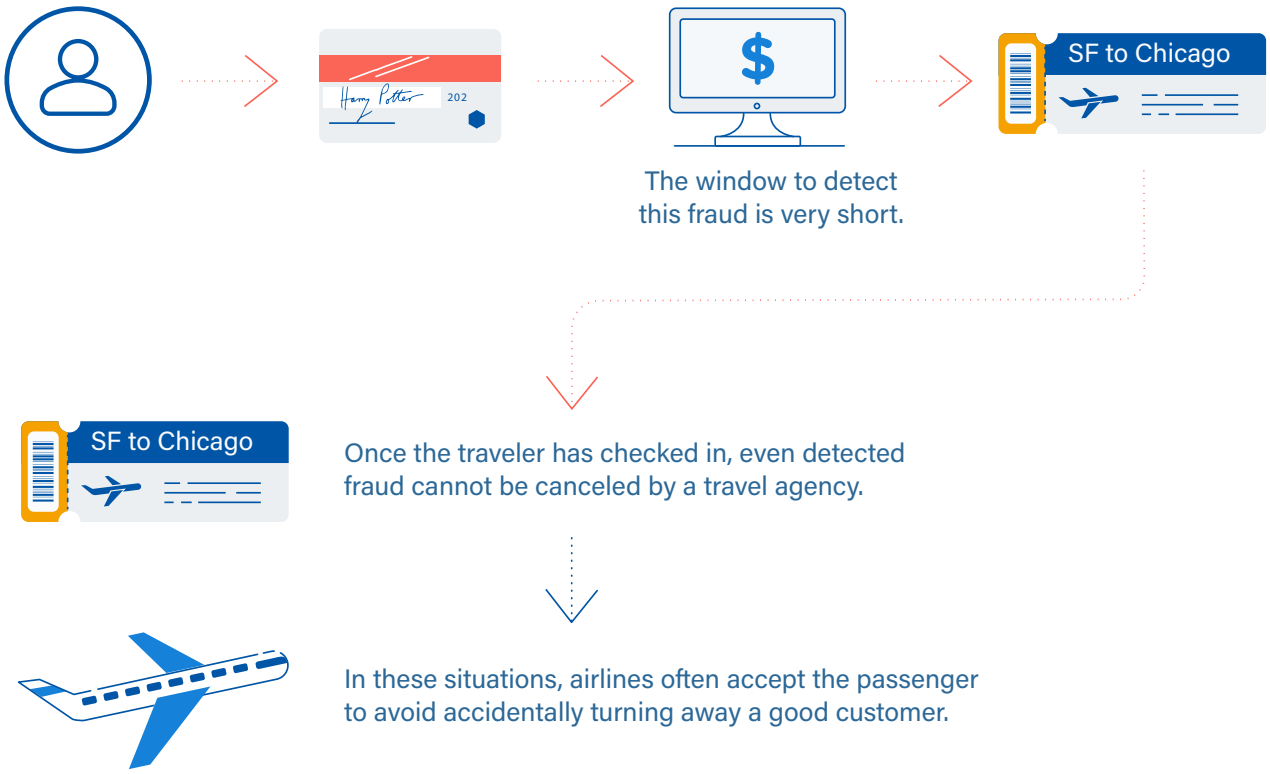
'Cashout fraud'

Fraudsters purchase last-minute, refundable airline tickets, train tickets or hotel rooms using stolen credit card information.



Immediate departures

Fraudsters purchase tickets with departure times 24-48 hours after purchase using stolen credit card information.



Loyalty program fraud: a growing problem for airlines and hotels

Account takeover (ATO) is a growing problem across many types of online businesses, including airline and hotel loyalty programs. One of the main drivers? Data breaches and compromised credentials are on the rise, yet 59% of consumers still reuse passwords across multiple sites. This makes it frighteningly easy for fraudsters to get access to a loyalty account.

An investigation by Connexions Loyalty found that travel accounts could be quite valuable on the dark web:

- Airline loyalty accounts: **$3.20-$208 each**
- Hotel loyalty accounts: **$1.50-$45 each** so a fraudster is often in the clear once they cash out or use the fraudulent ticket or room. The time between a fraudulent transaction and the expiration can be as little as a few hours, so companies are racing against the clock to detect and block a bad purchase.

Source: The Sun

Source: flyertalk

Americans belong to an average **2.6** travel loyalty programs

31% of Millennials belong to 3+ travel loyalty programs

Source: Deloitte

$40B of travel and airline points sit unredeemed

Source: Gartner

70% of airline loyalty programs face fraud

30% of programs say the problem is increasing

Source: Airline Information

59% of people reuse passwords across multiple sites

Source: Password Boss

How loyalty program fraud works

Fraudsters get access to stolen credentials from a number of sources:

- From data breaches, sold on the dark web
- Phishing with fake websites
- Malware, trojans, spyware
- Social engineering
- Hijacking a mobile device

Research from Airline Information revealed that a common loyalty fraud scenario takes place when a fraudster pretends to be a travel agent, then uses stolen miles, or miles bought with a stolen credit card, to buy tickets. Then they sell those tickets to real travelers.

In another scenario, a fraudster may use stolen credit card information to buy tickets in bulk, racking up thousands of points with an airline loyalty program. They quickly cash in or transfer the points, and the fraud is only discovered after the legitimate cardholder files a chargeback. In this case, the airline is out the cost of the ticket, the chargeback fees, and the value of the loyalty points.

The cost of ATO to travel companies can be measured in terms of revenue loss, operational costs, and brand damage. This price includes:

- Chargebacks
- Product replacement
- Reduced engagement
- Customer churn
- Negative PR
- Brand erosion
- Legal problems
- Compliance issues
- Ops, Eng & PM staffing

Loyalty accounts are an easy target

There is a thriving black market that exists solely for selling stolen loyalty points at a discounted cost. Many loyalty programs make it easy for the account holder to exchange their points for a variety of goods (including merchandise with a high resale value), services, and gift cards. Once fraudsters access an account, they quickly use up any stored value without ever having to enter another form of payment or other information. They may also use their account access to get a hold of consumers' payment information and sensitive personal data.

One challenge in preventing ATO of loyalty accounts is that many travelers who join loyalty programs are passive about maintaining, redeeming, or checking those accounts. They may have stored up a significant amount of value, yet these same consumers overlook the security of those accounts since points don't feel like "real" cash.

How travel companies traditionally tackle fraud

Understandably, travel companies are devoting budgets and humans to combating fraud. The problem? Too many travel businesses are optimizing to lower fraud. But these tactics come at the expense of growth and positive customer relationships. Plus, it's expensive to maintain older systems.

The bottom line: companies need to deliver on these high expectations, without increasing risk.

> "Consumers want authenticity, personalization, removal of friction, and on-demand functionality in their travel experiences."

Deloitte 2017 Travel and Hospitality Industry Outlook

Legacy solution #1: Create rules

In the past, travel companies implemented rigid rules engines to combat fraud. This approach can appear to be successful if the fraud attacks you're facing are fairly simple. However, fraudsters are evolving, their methods are growing increasingly sophisticated, and they're getting better at disguising their behavior to look like that of legitimate users.

There are a number of ways in which rules come up short, including:

Rules aren't accurate

Rules treat the world as though it's black and white, leading to both false positives and false negatives. Turning away good users means lost revenue, and accepting bad users leads to more loss. Unnecessary manual review is also a big operational cost that prevents your team from focusing on higher ticket tasks.

Rules don't adapt

Staying ahead of fraudsters is impossible because rules never match their step. By the time the source of a new pattern has been identified, bad accounts, orders, and content have already gone through.

Rules don't scale

Many legacy rules systems require several months of integration and tuning before they deliver anything close to accurate results. Beyond that, they require constant evaluation and updates, and their numbers pile up quickly. You end up with hundreds of rules that you can neither keep track of nor easily scale back if they are ineffective.

Legacy solution #2: Introduce 3D Secure and other verifications

Many companies view 3D Secure — a security step that requires customers to enter a password to verify their identity — as an added layer of security. But when used too liberally, it can become an impediment to conversion. Not only does 3D Secure require users to remember and correctly enter an additional data point, but this user experience is not well-suited to the mobile channel and is an additional cost for the company.

Historically, travel companies – particularly airlines – have over-relied on 3D Secure to the detriment of their conversion rate. The same goes for Captchas, two-factor authentication, and other checkpoints aimed at verifying a user's identity.

When introducing a new verification step, it's important to use it judiciously and even dynamically. That's why innovative companies, where marketing and fraud teams are aligned towards the goal of maximizing conversions, are embracing solutions that allow them to automatically adjust the user experience based on risk score. That way, only the riskiest users are asked to complete an additional step on their way to a successful purchase.

As many as **31%** **of travel companies** use 3D Secure for every purchase.

Source: Airline Information

Legacy solution #3: Build out manual review teams

While many companies with a burgeoning fraud problem may address it by hiring people to manually review orders, they eventually discover that manual review is expensive and hard to scale. According to the 2017 Sift Fraud-Fighting Trends survey, 60% of online businesses are concerned about spending too much on manual review.

The average merchant dedicates six employees to manual review with a median review rate of 15 orders per hour, according to the latest Merchant Risk Council (MRC) data. "To deliver a more responsive customer experience, merchants should explore tools and processes that can accelerate that rate," the MRC recommends.

One major OTA using Sift generated **$120K** in monthly gross profit when they began diverting fewer transactions to 3D Secure.

Why legacy fraud-prevention solutions come up short

Payment fraud and loyalty program fraud have been rampant in the travel industry, yet many companies are still relying on an outdated and reactive fraud prevention approach. With higher-value purchases at stake, some companies have been hesitant to move on from legacy rules systems to layer on a machine learning approach. The result? Higher rejection rates, an unnecessary and expensive reliance on two-factor authentication, and more customer insults. Fraud prevention directly impacts their top line.

Why are companies so hesitant to switch? An organization may have already invested significant time and money into developing a system of weighted rules. It could feel intimidating to consider giving that up for an unfamiliar approach that can feel like a "black box." And they may not want to face a sunk cost.

Here's a quick table listing the pros and cons of each approach:

Machine Learning	Rules
Proactive - tells you what's happening	Reactive - tells you what already happened
Learn across many data elements	Limited data elements
Scalable	Higher maintenance
Needs statistical significance	Can operate on a small data set
More accuracy at scale	Less accuracy at scale

Machine learning: why it's ideal for protecting and growing your travel business

While rules may still be used to prevent fraud today, machine learning is gaining prominence as a more nimble approach advanced by forward thinking travel companies. The quantum leap in computing and big data power, as well as the increase in API-based machine learning solutions, mean that machine learning can now be leveraged by any company looking for a scalable way to grow without increasing risk. Industry leaders are leveraging machine learning to increase their top line and expand into new markets while keeping fraud at bay.

High accuracy

Humans can't possibly stay on top of fraudsters by constantly adapting tactics, adjusting rules, and keeping them accurate. Machine learning, by contrast, recognizes patterns in data that aren't easily detectable by humans. This leads to fewer false positives and false negatives.

Ability to positively alter the user experience

Machine learning systems are not just good for identifying and stopping bad behavior. They can also be used to identify good users, so you can dynamically adjust their experience.

Real-time decisions

To stay ahead of fraudsters, travel companies need to gain actionable intelligence from all possible data inputs instantaneously, so you can act as quickly as possible. Machine learning analyzes huge volumes and varieties of data to deliver real-time decisions, without sacrificing accuracy.

What is machine learning?

Machine learning refers to the practice of training computers to recognize patterns and make predictions. A machine learning system can learn, predict, and make decisions without being programmed.

Similar to how email spam filters learn to recognize which messages to deliver to your inbox, a machine learning system can distinguish the characteristics of fraudulent purchases from legitimate ones.

Machine learning is often deployed as part of automated fraud screening systems, identifying high-risk transactions, accounts, and risky logins to prevent payment fraud, account abuse, and account takeover. Machine learning can replace even the most complex rules set and produce higher accuracy, fewer false positives, and savings through automation.

Adaptability

Machine learning models are capable of continuous learning, adapting to sudden changes in fraudsters' strategies. With a steady stream of quality data and feedback, a machine learning system's predictions will get more and more accurate.

Automation-friendliness

Data from LexisNexis reveals that merchants spend up to one-quarter of their fraud prevention budget on manual review. Machine learning enables teams to automate tasks that don't necessitate human review. This provides an efficient, streamlined process that saves you money and valuable time.

Network effects

Machine learning systems that draw upon a global network of data allow that data to be shared – and increase your chance of identifying emerging threats before they even reach your site. With Sift, our real-time machine learning reevaluates your risk every time a user takes action on any site or app across our network.

High-volume data ingestion

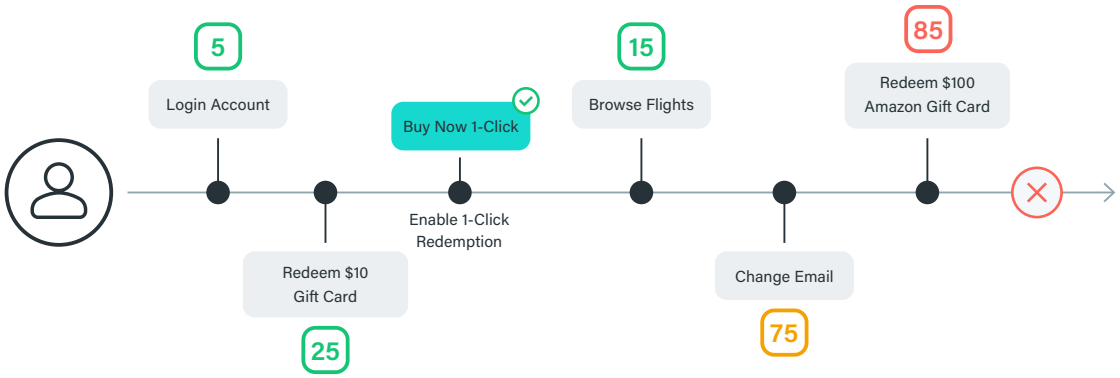
Machine learning can take in a huge amount of data. The important thing to know is that so much of this is passive data based on user behavior.

How does a legitimate customer's behavior differ from a fraudster's? For example, a traveler browsing a site may do multiple searches, spending time comparing a bunch of different options.

They might return to the site many times, or forward a suggested itinerary to a friend. The typical transaction time will be hours long. A fraudster is likely to spend less time, and complete many fewer of each of these actions.

At Sift, we have over 16,000 signals we look at. Here are just a few examples:

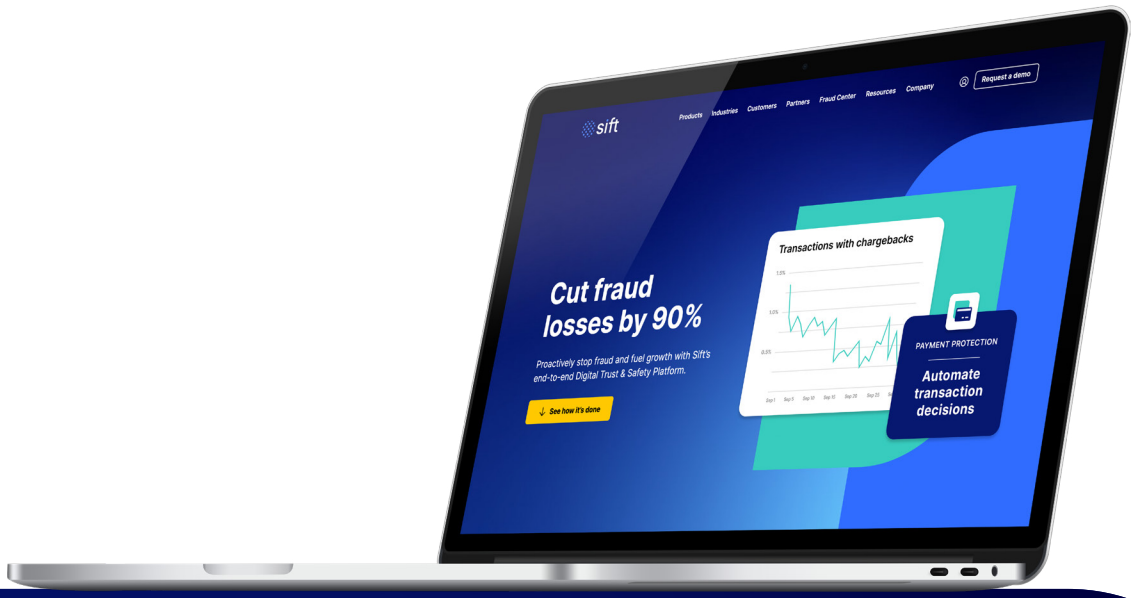
- Account age
- Time until event
- Seat selection
- Order size
- Destination
- Buyer location
- Device type / ID
- Fare class



The Sift Digital Trust Platform for travel companies

Machine learning is being widely used to prevent fraud and increase revenue, but not all machine learning systems are created equal. The fastest-growing trust platform in the travel industry, Sift prevents fraud and increases revenue for top travel companies around the world.

We are the only company to use real-time machine learning, automatically utilizing learnings from our global network of customers, as well as your own data, to provide a clear view of good and bad users. This lets you reduce checkout friction and the need for costly authentication systems. Sift is ideal for growing companies and enterprises, offering a holistic solution that can solve multiple fraud problems through a single integration.



End-to-end intelligent automation with Sift

Sift is the leader in Digital Trust & Safety, empowering companies of every size to unlock new revenue without risk. Our cutting-edge platform dynamically prevents all types of online fraud and abuse with intelligent automation that adapts based on Sift's unrivaled global data network of 70 billion events per month. Global brands including Twitter, DoorDash, and Wayfair rely on Sift to catalyze growth and stop fraud before it starts.

Visit us at sift.com and follow us on LinkedIn.

> "Sift is a real-time learning system that adapts quickly and gives us accurate results. With Sift, you can discover trends more quickly."

Gaspar Salva
Revenue Protection Analyst

LOGITRAVEL

Logitravel, an international OTA based in Spain, found that the rules-based solution they were using couldn't keep up with their company's growth. They chose Sift for its accuracy and ability to learn in real time.

Case Study

> "Traditional rules-based solutions require that you are always reactive, instead of proactive. With machine learning, we're more proactive and we're staying ahead of the fraudsters."

Gustavo Tonti
Fraud Manager

destinia

Destinia, an OTA operating across more than 90 markets, was looking for an advanced technology to optimize manual review, fight fraud, and increase conversion.

Case Study

> "Sift helps us to identify more good customers and reduce the number of transactions that have to be authenticated, thus reducing payment friction and increasing overall conversion."

Wayan Tresna Perdana
Sr. Product manager

traveloka

Traveloka, the top travel booking platform in Southeast Asia, found that their in-house rules system was generating too many false positives. They turned to Sift's machine learning as a flexible and adaptive solution.

Case Study

For more information, visit sift.com/travel or contact sales@sift.com.