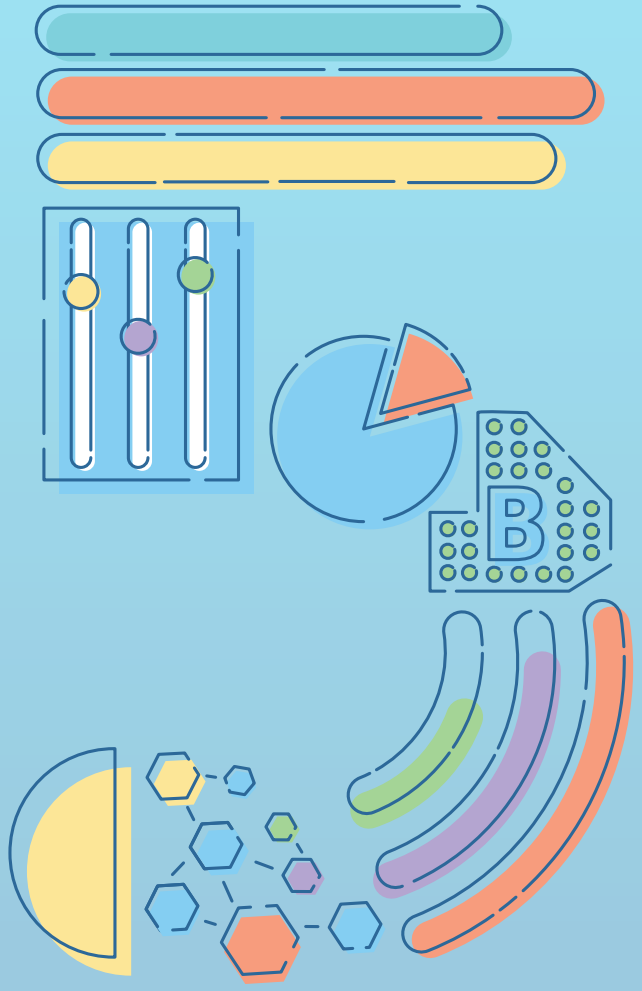


Trends Redefining Fraud

sift science

Contents

Another ebook about fraud?

In the minute it takes you to read this paragraph, nearly 4,000 people will fall victim to fraud. That's about 60 passwords, email addresses, credit card numbers, or security questions stolen each second – impossible for even the sharpest fraud analyst to keep up with. When fraud happens that fast, it can start to feel overwhelming. No one has time to try and find patterns in the data breaches and account takeovers. If you don't have a smart fraud tool, you'll start to rely on reflex, not strategy. You'll get lost in the weeds.

That's where this ebook comes in. This isn't just another ebook about fraud: it's a guide to help you navigate your business through obstacles and next steps. We've pored over the data, sorted through the news, and interviewed experts and (former) fraudsters. Our goal? To narrow down five themes currently underpinning the world of fraud. **Armed with insights about these 5 trends, you can build a strategy that helps you delight and retain customers while growing your business**. Whether you're planning for the next month, quarter, or year, this ebook can be your guide.

How to use this ebook

Each section of this ebook is divided into three parts. Here's how you can use each part as a resource as you guide your business into the next quarter.

What's the theme and why does it matter for my business?

We've gotten the scoop from leading industry experts with insights into unique fraud challenges. Use this section as a reference as you're thinking about what to prioritize and where to allocate resources.

How is this theme relevant to my business?

To ground these themes in the real world, we've highlighted relevant stats and salient news headlines.

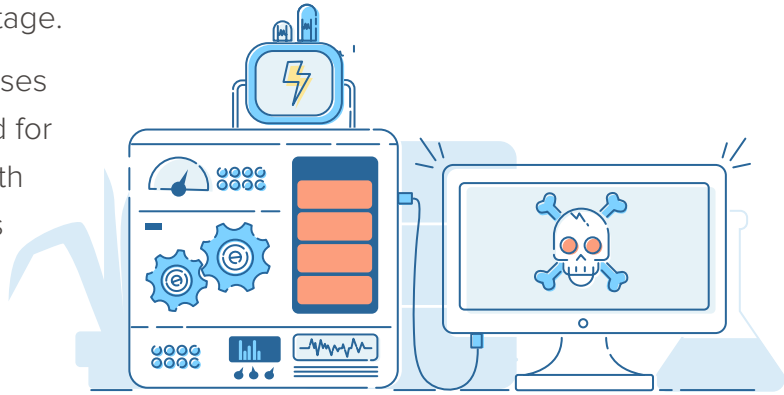
What steps can I take to protect my customers and bottom line?

We close each section with a to-do list.
These suggestions are designed to help you take actionable steps to respond to potential obstacles.

1 An uphill battle

Fraudsters are using our own fraud-fighting technology against us.

We're fraud-fighters, which means our goal is to make fraudsters' lives as difficult as possible. And it works...some of the time. According to Brett Johnson, a former FBI Most Wanted hacker, an alarming trend has emerged. Cybercriminals have started to learn from fraud-fighters. They're appropriating our tools, techniques, and methods for their own nefarious aims. And as it turns out, fraudsters have a key advantage.



Cybercriminals are unencumbered by the rules and norms that keep businesses and anti-fraud companies from sharing information. Existing laws make it hard for bug bounty hunters and white hat hackers to share website vulnerabilities with affected businesses. Regulations, privacy policies, company rules, and norms make it similarly hard for merchants to share information with each other.

But Brett says criminals aren't like that. When fraudsters learn about new tech, they share freely, test their techniques, and build on each other's strengths. Ethics don't get in their way, so they can share without consideration for regulations and proprietary technology.

The flow of information on the dark web has allowed fraudsters to build a sophisticated repertoire of tools that draws heavily on our own fraud-fighting methods: device fingerprinting, machine learning techniques, and more. Brett says this partially accounts for the sharp rise in account takeover over recent years.

> "It's important for companies and the anti-fraud industry to understand just how sophisticated criminals are – not just the crimes themselves, but the network."

Brett Johnson
Former FBI Most Wanted hacker

Account takeover by the numbers

48% of businesses experienced a rise in ATO in 2016

$5.1 billion was lost to ATO in 2017

$290 is the average victims pay to resolve ATO

Sift Science, Javelin Strategy and Research

How are criminals using fraud-fighting technology to commit fraud?

1. Using device ID to look legitimate

A device ID is a unique identifier assigned to a smartphone or similar device. Fraud fighters use device IDs and other fingerprints to adjudicate between suspicious and honest users. But according to Brett, fraudsters now sell device IDs on the dark web. Their behavior is less likely to raise red flags when they hide behind an "honest" device ID. Fraudsters also sell credit card numbers and passwords with honest users' device fingerprints attached to them.

This might become even more of a problem as legitimate users and fraudsters start to look more alike. For example, Apple just debuted privacy settings that may make legitimate users harder to track. As privacy becomes more of a selling point for browsers and devices, fraudsters will continue to reap the benefits.

2. Using machine learning to customize phishing emails

Businesses increasingly rely on machine learning (ML) techniques to fight fraudsters. We're constantly improving ML systems to make fraudsters easier to identify and catch. But fraudsters are benefitting from these innovations, too. Sophisticated criminals are starting to develop ML tools that allow them to expertly customize phishing emails. Fraudsters draw on publicly available data and market trends to craft phishing emails tailored to their victims, as well as to identify which employees are most likely to fall victim to phishing scams.

3. Using a SOCKS5 proxy to emulate honest users

Socket Secure, or SOCKS, is an internet protocol that allows data to pass between a client and server via a proxy server. SOCKS5 is a method of authentication: it only permits authorized users to access a server. Brett has found that cybercriminals now know how to harness the power of SOCKS5 proxy servers. The SOCKS5 proxy acts as a buffer between systems, so fraudsters can use the proxy to hide their true IP address, physical address, device ID, and more.

4. Using machine learning to create complex malware

Businesses and fraud fighters have long used ML to detect malware. But sources within the hacker community say fraudsters are figuring out how to reverse engineer ML tools to improve malware. Stay with me, because this one can give you a headache: The fraudsters' ML system learns what the fraud fighters' ML system is observing. In doing so, the fraudsters can make their malware more effective.

5. Using background checks and PII to steal identities

Many e-commerce sites rely on personally identifiable information (PII) like Social Security numbers, passwords, and security questions to verify users' identities. But Brett says any fraudster can leverage PII to steal someone's whole identity. Fraudsters can pay a few bucks for PII on the dark web, or they can go through someone's social media profile to find out their date of birth, mother's maiden name, the name of their elementary school, and other info; this has become so easy that some have started pushing for users to lie on security questions. Once they have the victim's Social Security number, date of birth, and address, they can proceed to the next step.

The fraudster then uses a standard background check program to get the victim's credit report. That's where it gets really devious, Brett says. The fraudster calls the utility company their victim is using and ask the company to update their billing info. Brett says that's usually easy to do, since no one expects a criminal to defraud a utility company. Adding the fraudster's billing info to the utility company simultaneously adds it to the credit report. Then the fraudster can set up new bank accounts, order replacement cards, and more under the victim's name... without setting off any red flags.

6. Using cookies to take advantage of stolen credit card numbers

E-commerce sites use cookies to keep track of information as a user interacts with the site. Fraud analysts often use cookies as tools that flag anything suspicious, like when a repeat customer changes their billing address. But fraudsters have learned how to game the cookie system. After stealing credit card info, fraudsters can hop into an e-commerce site and put something in the cart. That creates a cookie. They then "age the cookie," as Brett puts it, by leaving the item in the cart for a few hours. The fraudster can then change the billing address without raising any red flags.

> With just a password and login, a savvy criminal can take over someone's entire online life.

Brett Johnson
Former FBI Most Wanted hacker

Your to-do list

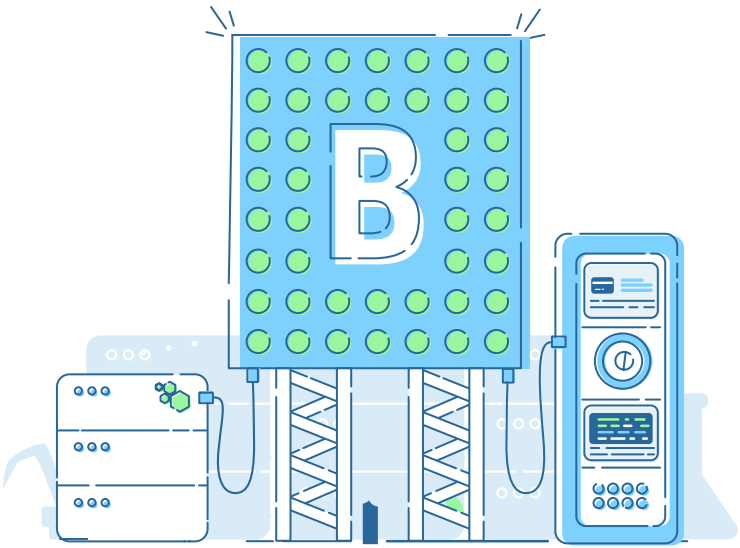
- If you are using an external fraud prevention solution, ask them what they're doing to respond to new threats
- Be open to (legitimate!) bug bounty hunters like those at HackerOne who try to contact you about vulnerabilities on your site
- Share trust & safety learnings and best practices at merchant conferences, industry meetups, and online forums
- Make sure your employees and network maintain an open line of communication about fraud
- Train your employees to recognize phishing emails and other fraud tactics

2 New kid on the block(chain)

Cryptocurrencies and the blockchain are the newest fraud frontier – driving more fraud than ever, or helping to stop it.

Since bitcoin was created nearly ten years ago, cryptocurrencies have experienced a startling evolution: from a fringe investment to a mainstream medium of exchange. Enterprising fraudsters have been following this evolution closely. **In the first two months of this year, cryptocurrency fraud has amounted to a $1.36 billion loss**. That's about $9 million lost per day. Despite these staggering numbers, few businesses or consumers understand how cryptocurrency is changing the face of trust & safety on the internet. Sift has long argued that trust is the currency driving the way we interact online.

With cryptocurrencies like bitcoin, trust quite literally *is* currency. Indexes are popping up that literally treat it as such. Patrick Presto, a researcher at NYU, explains that people who participate in cryptocurrency exchanges are using a decentralized system. Unlike standard banks, which are subject to government oversight, cryptocurrencies rely on a public ledger called a blockchain. Users rely on each other to maintain the blockchain, validating and timestamping transactions. But what happens when that trust is broken? And can we harness the blockchain to protect against fraud and abuse?



> "Even though cryptocurrency fraud is a new kind of online fraud, trust is still fundamental to everything."

Patrick Presto
Researcher at NYU

Cryptocurrency fraud by the numbers

80% of all coin offerings (ICOs) are scams

In the UK, bitcoin-related online scams **more than doubled** between 2016 and 2017

Fraudsters stole **$534 million** from cryptocurrency giant Coincheck

The Coincheck scam affected **260,000** customers

Why should you care?

1. Cryptocurrency fraud is spreading.

Even if you'd never heard the term "ICO" before reading this sentence, you and your customers are vulnerable. In early May of this year, fraudsters hacked into more than 400 business, government, and university websites, surreptitiously turning them into cryptocurrency mining platforms. Crypto mining is a huge investment of electricity and computing power, so the fraudsters drained their victims' CPU resources before moving onto their next victim. That's right: drive-by data mining.

And that's not all. According to Daniel Sankey, compliance officer at Coinbase, fraudsters are increasingly turning to bitcoin to put a new spin on old schemes. Scammers often earn victims' trust in romance scams – for example, convincing a user on a dating site that they're interested in a relationship – before demanding payment in the form of bitcoin or other cryptocurrencies. Fraudsters have become adept at targeting vulnerable users, organizations, businesses, or government entities that don't have sophisticated malware filters, but that do have money. Especially worrisome: they tend to target entities like hospitals or government agencies, which desperately need access to their files, and then they hold the files ransom for bitcoin.

2. The technology underpinning cryptocurrencies and the blockchain could be our next line of defense against fraud.

The past few years have shown us that firewalls, encryption, and intrusion detection systems aren't enough to keep fraudsters from stealing massive amounts of data. We're living in a post-Equifax world, in which data breaches are a fact of life. But maybe they don't have to be. Fraud fighters are beginning to explore how the technology underpinning cryptocurrencies and the blockchain might be used to protect users' data.

Security engineer Diogo Mónica recently put a name to an IT architecture idea that may help safeguard user data. "Crypto Anchors," which Mónica and his colleague Nathan McCauley developed at Square, work like this: The system encrypts database contents using a key stored on a single-purpose computer called a Hardware Security Module, or HSM. Let's say a fraudster tries to access that database. The HSM acts a gatekeeper that decrypts each record one-by-one. Businesses can configure the HSM to throttle its decryptions so the data can't be unscrambled faster than a fixed rate.

The implication here is really cool. Even if a hacker takes over a computer on a corporate network that has access to a database, they can't just do a hit-and-run, stealing the data and fleeing. The fraudsters stay "anchored" inside the database while they wait for the HSM to decrypt each piece of data. That can take months or years, during which the fraudsters' presence remains visible on the network.

Mónica and McCauley aren't the only ones looking to cryptocurrencies and the blockchain for innovative fraud solutions. Vinny Lingham, CEO of Civic, aims to leverage Bitcoin's blockchain to create an offline model of identity management. When a user signs up for the Civic app, Civic collects the user's identifying information. The information is passed through a verification service, usually a government agency or third party. Then Civic takes a cryptographic hash of that information. They apply an algorithm that translates that information into a unique set of numbers called a signature. This process is called cryptographic hashing. Civic inserts that hash into the public blockchain before erasing the user's personal data from their servers.

Say the user needs to verify their identity before making a purchase on an e-commerce site. Maybe they have to answer a security question about the name of their elementary school before they can continue. When the user shares that information with a site, the information is sent through Civic's algorithm and checked against the hash on the blockchain. Once the user has verified their identity, neither Civic nor the business using Civic needs to store their information.

> "Fraudsters are smart. They know to target vulnerable entities that don't have sophisticated malware, but that do have money. Then they hold their files ransom and demand bitcoin."

Daniel Sankey
Compliance Officer at Coinbase

To summarize all that, Civic can confirm your identity without holding onto your personal information. If Civic or a business using Civic experiences a data breach, there's nothing to steal. All your personal information is encrypted on the blockchain.

3. Fraudulent ICOs erode trust.

Cryptocurrencies start with an ICO, or initial coin offering. That's a round of public funding in which investors buy coins with the hope that they'll increase in value when the company launches its product. According to ICO advisory firm Static Group, about 80% of ICOs are scams.

Why does that matter if you're not buying tokens in an ICO? Simple: fraudulent ICOs erode trust. As more cryptocurrency changes hands, there's always a chance ordinary internet users will become suspicious of the information they see online. On the internet, uncertainty breeds uncertainty. If you're in charge of an online marketplace or community, you'll be impacted.

> "With cryptocurrency fraud, the more things change, the more things stay the same."

Patrick Presto
Researcher at NYU

Your to-do list

- If you accept cryptocurrencies as payment, make sure you know exactly how you're storing your crypto and set up defenses accordingly
- Be transparent and communicative with your users when you decide to introduce crypto as a payment method
- To make sure your crypto isn't passing through (or from) the hands of fraudsters, consider using a vendor that analyzes signals to detect fraudulent behavior

Compliance, compliance, compliance

GDPR was only the beginning.

By now, you're more familiar with GDPR than you ever wanted to be – whether it's because of the countless emails about updated privacy policies that are still sitting in your inbox, or because your business had to do some updating and emailing too. Enforcement of GDPR, the European Union's General Data Protection Regulation, started on May 25th 2018. **Every company that processes EU citizens' data must comply, so pretty much everyone has been impacted**.

How did we get here?

According to a survey of consumers in France, Germany, Italy, the UK, and the US...

62% say they blame businesses, not fraudsters, for data breaches

41% say they intentionally falsify data when signing up for online services

72% say they would boycott a company that seemed to disregard the protection of their data

50% say they would be more likely to shop at a company that could prove it takes data protection seriously

Source

Although the sky didn't fall on May 26th, we can't underestimate the impact of GDPR. **Governments worldwide are grappling with privacy regulation**, struggling to understand what businesses can (and should) do with consumer data.

And businesses are struggling too: trying secure customers' trust by laying the groundwork for compliance, but not burdening users with opt-ins, notifications, restrictions, and other hassles.

For more insight, we spoke to Jeff Sakasegawa, a trust & safety architect at Sift Science who used to handle compliance at Square. Jeff says that these regulations can be unexpectedly great for your business. **If you play your cards right, compliance initiatives like GDPR give you a great opportunity to prepare your business for a world in which data is currency**, and data protection makes or breaks consumer trust. If you don't, you'll fall behind. Regardless, though, one thing is clear: GDPR wasn't the end of the story.

It's not just GDPR

If you thought you were done with compliance on May 26th, think again. Trust is playing an increasingly central role in the way we operate online, and compliance gets second billing.

PSD2, the EU's directive on payment services, is another sign of things to come. Designed to incentivize fraud prevention and disrupt trends in online banking, the Revised Payment Service Directive (PSD2) could prove to be a game-changer. Its effects are twofold.

First, to comply with PSD2, banks must release their data in a secure, standardized form that allows it to be shared between authorized online organizations. Banks have a lot of data; that's no surprise. They know about everything we spend, borrow, and give away. PSD2 makes it possible for banks to give this information to third parties, who can then use it to make new products. **The implications are clear: any entity that takes possession of that data – from Google to Facebook to smaller fintech companies – can now compete with a bank**.

If that sounds unsafe, don't panic. The second part of PSD2 is that banks can't share that information without explicit approval from the account holder. So, anytime an account holder accesses their account online, engages in a transaction, or performs an action that produces data which

> "Compared to something sexy like working on a new product launch, GDPR compliance is like eating your vegetables. But, like eating your vegetables, it could be good for you."

Jeff Sakasegawa
Trust & Safety Architect
at Sift Science

could be shared with a third party – anytime a user does anything at all, Strong Customer Authentication (SCA) is mandatory. SCA is a method for multi-factor authentication. It requires the user to validate their identity by providing knowledge that only they would know, like which middle school they attended, or their mother's maiden name. Yes, that's right: to comply with PSD2, **fraud prevention is no longer optional**.

GDPR and PSD2 are sending a clear message. **Businesses must invest in fraud prevention solutions that are robust, effective, and transparent**. Companies that failed to do so prior to GDPR and PSD2 found themselves scrambling and vulnerable when the regulatory hammer came down on their heads. Don't be that guy. Your customers will thank you.

> "Learn from your peers. Whatever industry you're in, there are probably interest groups, trade publications and conferences that are trying to educate their constituents on the GDPR and how it applies to their industry."

Jeff Sakasegawa
Trust & Safety Architect
at Sift Science

Your to-do list

- Invest in a robust fraud solution
- Make sure all your privacy policies are up to date
- Establish procedures for keeping your customers informed so that they're always aware of the data you're collecting and what you plan to do with it
- Audit the data you're collecting to make sure you are only collecting data in pursuit of the application you've told your customers about

4 Hang on, did a bot write this section?

The war on content abuse is getting harder to win.

What if this whole ebook is just an elaborate example of fraudulent content? We promise it's not...but it's getting harder to tell the difference! Content abuse has become so sophisticated that Gartner predicts **people will see fake information *more often* than true information online by the year 2022**. That includes material as alarming as fake videos.

Any online marketplace or community that's powered by user-generated content (UGC) is vulnerable to content abuse. UGC can include comments, blog posts, marketplace listings, videos... Twitter, YouTube, Pinterest, Indeed, and AirBnB are built around UGC. **If content abuse drives users away from these sites, the whole business falls apart.**

UGC Drives E-commerce

UGC is 35% more memorable than other media

Customers spend 5.4 hours per day with UGC

User-generated YouTube videos get 10x more views than those uploaded by brands

UGC results in 29% higher web conversions than sites or ads without it

25% of search results for the world's 20 largest brands are links to UGC

But what's content abuse? Content abuse occurs when fraudsters create or share fake or malicious UGC. Unlike more cut-and-dry types of fraud like payment abuse, content abuse can take myriad forms: spam, fake listings, catfishing, fake reviews, and toxicity. That makes it a moving target. Content abuse has become such an insidious threat that the EU is considering a dizzying variety of solutions to fight back, everything from bots to blockchain. And it's not just your run-of-the-mill fraudsters who are committing content abuse: even merchants pay for fake reviews on sites like Amazon.

The evolution of content abuse

Each instance of content abuse is like a cancer cell: it's disguised to look like an ordinary cell, mutating as the situation demands. Once content abuse infects an online marketplace or community, it breeds more content abuse. Honest users flee the site as their trust in the community is eroded. Fraudsters who sense the site's vulnerability flock there to commit yet more content abuse. It's a vicious cycle.

To make matters worse, fraudsters seem to be getting smarter. They now rely on a diverse toolbox of methods like creating fake accounts, taking over honest users' accounts, and scripted bot attacks. Content abuse is harder to spot, harder to stop, and easier to overlook than ever.

We spoke Robbie Fritts, director of fraud and payments at Poshmark, to learn about the evolution of content abuse. Here's how fraudsters are responding to fraud fighters' attempts to fight this serious threat.

1. When you ban words and images that fraudsters are using to spread toxicity...

...they turn to coded language to hide their intent. That pineapple emoji might not be as innocent as you think. Content moderators often ban words or phrases that have been used to spread hateful speech or incite content fraud. But savvy fraudsters get around these bans by using slang, codes, and emojis to refer to sexually explicit content, ethnic groups, and even specific people.

> "Scammers are getting much subtler with how they're framing their messages because we've gotten so much better at identifying content fraud."

Robbie Fritts
Director of Fraud & Payments at Poshmark

© Sift Science. All rights reserved.

Even worse, there is no central database that indexes hateful speech and symbols, so even the definition of "hate speech" can be subject to question. Fraudsters may also switch to a different language so that the content moderators, who probably don't speak Hungarian, can't keep up. When fraudsters are changing languages and IP addresses – maybe using VPNs to switch identities – content abuse becomes even harder to fight.

2. When you keep an eye on new users to make sure they're not fraudsters...

...they lie in wait to commit content abuse. In the past, fraudsters would create new accounts explicitly for the purpose of committing abuse. As a result, sites often closely monitor new users' activities to make sure they aren't fraudsters, or they limited a new user's activities until the user is fully vetted. And while many still do commit fraud with new accounts, smarter fraudsters have found a workaround. They create an account, post innocuous content to lull the moderators into a false sense of security, and then they strike.

3. When you ban abusive content on the platform...

...they go off-platform and entice others to do the same. Many sites that rely on UGC have policies that forbid fraudulent content on the site. For obvious reasons, they don't have policies that forbid content abuse off the site. So scammers lure people into clicking on innocent-looking URLs that may lead to scams, attacks, toxicity, and other fraudulent content elsewhere. Fraudsters also may attempt an above-board transaction with a user on the site itself before luring them off-platform to pay for the service, possibly making illegal demands once the user is off the platform.

4. When you ban a single user who commits content abuse...

...they use machine learning to commit content abuse at scale. It's happened before. The most notable example was when the Federal Communications Commission opened their site to comments about net neutrality, and was flooded with content fraud created by bots. But it's happening elsewhere, as well; even sites like Google Maps are being inundated with content fraud powered by machine learning.

> "As we go forward, the main challenge is going to be responding to the evolving language that fraudsters use to commit content abuse online. Machine learning is going to become an even more important weapon in that fight."

Robbie Fritts
Director of Fraud & Payments at Poshmark

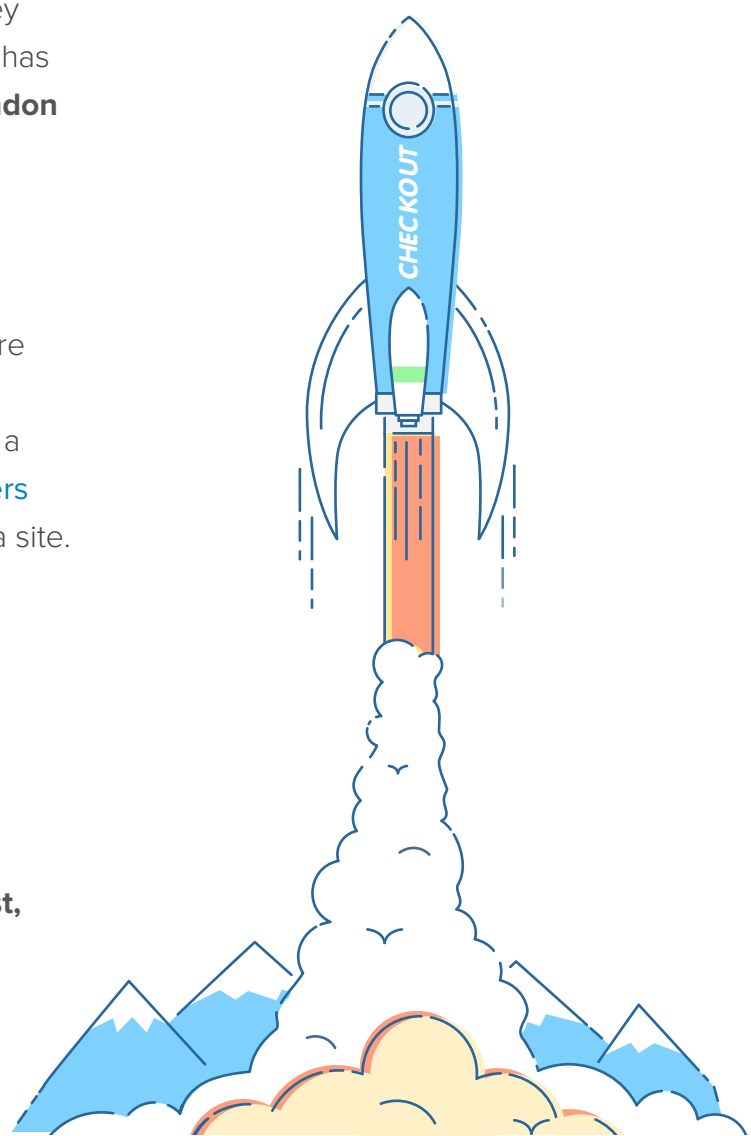
Your to-do list

- Ensure your content moderation team is up-to-date on content abuse trends
- Make sure your moderation team meets frequently to discuss best practices for fighting content abuse
- Allow your users to flag abusive content to decrease your moderation team's response time
- Update your terms of service so that it clearly and accurately reflects your standards as an online community
- Make sure your community guidelines and procedures for addressing abuse are visible to your users
- Consider investing in a machine learning solution to fight content abuse to keep pace with the speed and volume of fraudsters' activity

5 The battle for frictionless checkout

Maintaining a frictionless user experience while protecting user data is a perilous balancing act.

It's one of the most dreaded paradoxes of running an online business. Customers trust businesses to provide a frictionless user experience from start to finish. They want to get from the buy button to the "track shipment" page as quickly as possible. But they also trust businesses to keep their data secure. No one wants to shop at a site that has lost user data to fraudsters in the past. Customers are fickle creatures. **They'll abandon their cart if the checkout page requires repeated identity verification...but they also** won't shop at a business **that has suffered data breaches or other attacks.**



You're pushing my buttons

The fight to retain users has returned to a familiar battlefield: the Buy button. As more people rely on their computers (and phones!) to get their shopping done, the Buy button has taken on an almost mythic significance. Many e-commerce sites believe a simple, alluring Buy button decreases shopping cart abandonment. Indeed, shoppers universally cite a cumbersome checkout experience as a key reason they'll leave a site.

To many, this obsession over the Buy button can be traced to Amazon. Amazon pioneered One-Click ordering. You know the drill: you enter your credit card information and shipping address just once, after which you can order that impulse buy at the touch of a button. **Since consumers have come to expect an easy one-click experience, businesses are increasingly turning to companies like PayPal and Apple to provide something similar**.

Now that the One-Click patent has expired, Facebook, Twitter, Google, Pinterest, and others are jumping on the one-click bandwagon. Pinterest, for example, has implemented "buyable pins." To start, users enter their credit card number and

shipping address into the app. Pinterest relies on user-generated content drawn from thousands of retailers worldwide, so, when a user spots something they want to buy, they simply click “Buy it” – and the site sends their shipping and payment information to the relevant retailer. The buyable pin technology is supported by an external payment app, meaning it wasn’t developed (and isn’t maintained) in-house.

Why Do Users Abandon Their Cart?

The site wanted me to create an account - **37%**

The checkout process was too long or complicated - **28%**

I didn’t trust the site with my credit card information - **19%**

There weren’t enough payment methods - **8%**

Source

One button to rule them all

Here’s where it gets really interesting. Visa and MasterCard are planning to combine their Visa Checkout and Masterpass options into a single button: the so-called “universal Buy button.” American Express and Discover will also join in. **The companies aim to compete against one-click payment giants like PayPal and Amazon**. Websites that accept the universal Buy button will be cashing in on the ultimate frictionless checkout experience.

What does this have to do with fraud?

According to Karisse Hendrick, fraud consultant and market evangelist at CardNotPresent.com, frictionless checkout may not be as risk-free as you'd hope. You may be annoying users by forcing them to create an account and enter their information on your site...but you're also gathering invaluable data. **That data helps you identify fraudsters and makes it easier to deal with potential chargebacks down the road**. Karisse says losing access to that data could leave your business vulnerable to attacks. It could hit your bottom line, and hard.

External payment apps like Apple Pay, Google Pay, PayPal, One-Click, and eventually the "universal Buy button" pose a serious problem, says Karisse. If you've blacklisted a fraudster on your site, there's nothing to stop them from using an external app to commit fraud. The universal Buy button might make it easier for fraudsters to disguise their identities and pose as honest users. Fraudsters typically add stolen credit cards to their e-commerce account to test the cards or make large purchases, which often flags your system and prompts a fraud analyst to investigate. But fraudsters can leverage external payment apps to add stolen credit cards without setting off any red flags. Sure, a frictionless checkout experience *could* entice more shoppers to engage with your site, but it may end up enticing fraudsters, too.

The problem starts from square one. As Karisse points out, the fraud department doesn't usually make decisions about payment methods. Companies like Visa and MasterCard provide incentives for a company to use their payment method to streamline their checkout experience. What does that mean for fraud? **It means that adopting a new payment method is typically a *marketing* decision, not a *trust & safety* decision** – and the fraud department doesn't hear about it until they have to deal with the fraud.

> "There's a huge gaping hole that fraud can get through. These external payment apps might be the culprit."

Karisse Hendrick
Fraud Consultant and Market Evangelist at CardNotPresent.com

The bottom line? If you're an e-commerce retailer, the universal Buy button is one to watch. Customers expect an easy and pleasant checkout experience, and the universal Buy button promises exactly that. But this balancing act – frictionless user experience versus user safety – isn't going away anytime soon. In fact, it's only going to get trickier.

> "The less friction you put in place, the easier it is to commit fraud — and when you're relying on another company to make fraud decisions, you're missing out on really important data that you need to make the right choices for your business."

Karisse Hendrick
Fraud Consultant and Market Evangelist at CardNotPresent.com

Your to-do list

- Make sure your fraud team is briefed on any new payment methods your business may accept
- Consider investing in a machine learning fraud solution that determines a given user's trustworthiness and adjusts the checkout experience accordingly
- If you use an external payment app, see what steps they are willing to take to reduce fraud on your site