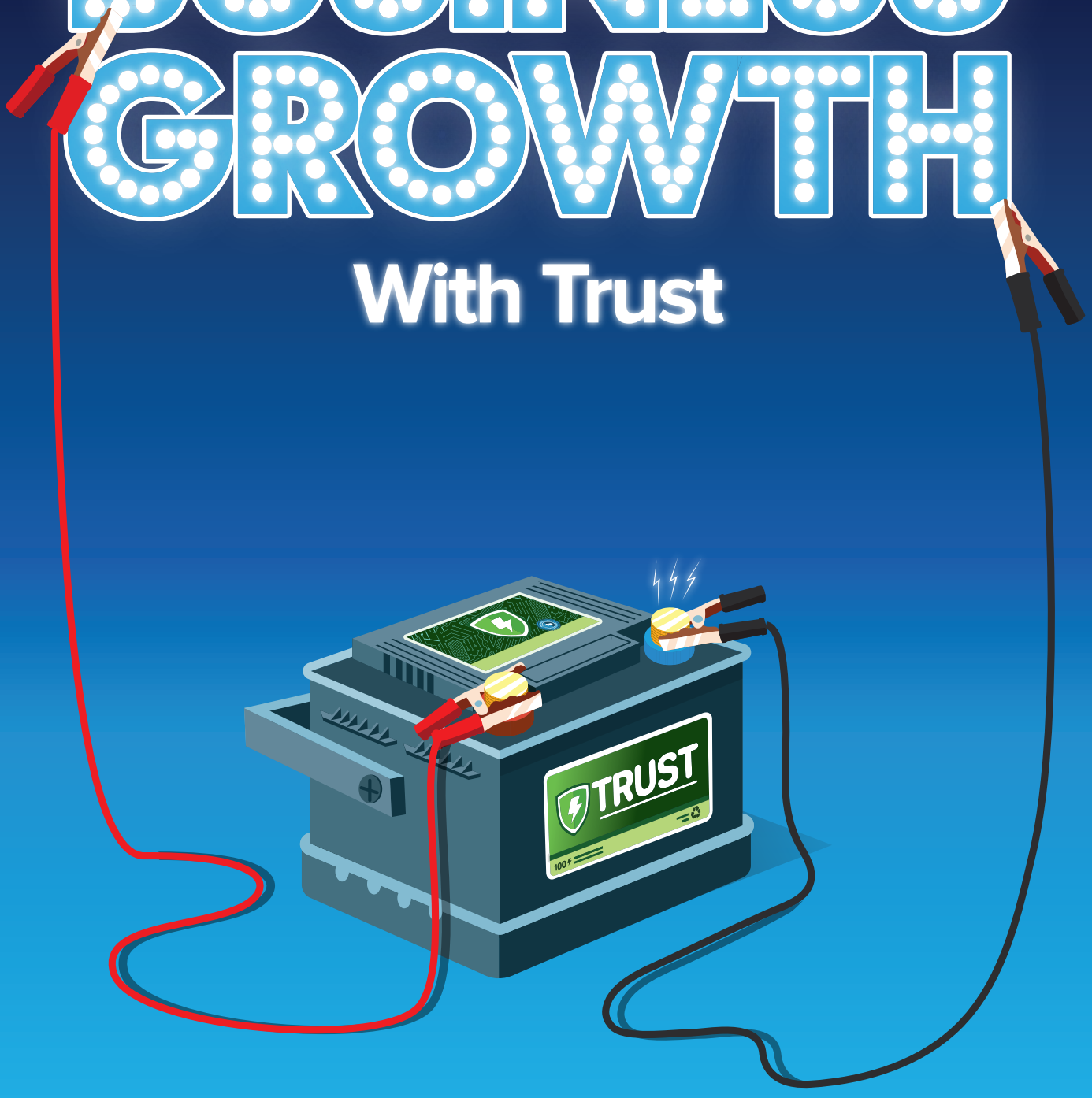
Power Your BUSINESS GROWTH With Trust



sift science

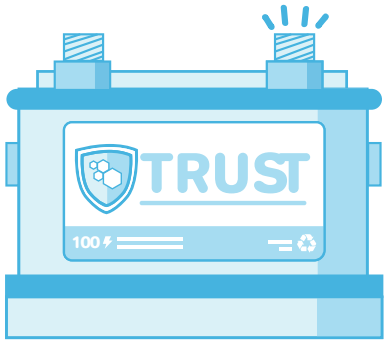
Why trust matters

When I say “airport stress,” what comes to mind? Lugging suitcases across terminals? Flights canceled at the last minute? For many people, the first image that pops up is going through security. We’ve all had moments when we’re shoeless, watching our wallets and phones travel precariously down a conveyer belt, being patted down by a stranger, when we’ve wanted to protest, “But I’m not doing anything wrong!!” You may not be plotting a criminal act, but the TSA system treats you like you are. It’s like every traveler is assumed guilty until proven innocent.

While we’d all like to be granted the trust we believe we deserve, and avoid the hassle of the airport security process along the way, it’s also easy to appreciate the challenge faced by the TSA. Essentially, they are balancing risk with traveler experience. A single malicious person can cause – and has caused – incredible damage and harm. Their priority is to make sure that doesn’t happen again. If only there were an easy, accurate, and inexpensive way to proactively and correctly identify that person, without impacting the experience of all of the legitimate travelers waiting in line. We could all enjoy the simple luxury of stress-free travel.

Airport security is a clear example of how an organization can inadvertently create an atmosphere of distrust in the name of mitigating risk. But what about the inverse – when you enjoy an experience where you feel completely and utterly trusted? Maybe your regular barista lets you pay later because you left your wallet at home. Or the security guard at your office allows you to board the elevator without bothering to show ID. For many of us, the role of trust in daily life is so fundamental, so ingrained in everything we do, that it’s easy to overlook – until you’ve been denied it.

Online, as you go about your digital day, you also take advantage of an invisible layer of trust – enabled by sophisticated technology – that allows you to transact and interact with as little interruption as possible. Every time you use your phone to quickly and easily order a ride with a simple tap. Every time you list an item for sale on a classifieds site without having to prove you’re not a scammer. Each comment you post on a friend’s baby photos where you don’t have to confirm that you’re not a robot.



Trust is the digital currency of the internet, enabling the flow of goods, services, and information online. Every single website that sells goods or services, every site that provides a platform for people to exchange things or ideas, must also make hundreds – or even thousands – of “trust decisions” every single day. But what is a trust decision? Basically, it all boils down to answering a simple question: Can I trust this user?

Fraud and abuse: a broader problem than ever before

There was a time when the description of “online fraud” was fairly straightforward (using a stolen credit card to make a purchase) as was the solution for stopping it (study the fraudulent behavior and set up business logic to prevent it from happening again). But new business models and rapidly changing technology mean fraud and abuse affect a wider swathe of businesses, in a wider variety of ways, than ever before.

Let’s walk through some of the ways that different businesses may interpret the fundamental question of “Can I trust this user?”, based on their business model, goals, and priorities.

Payment fraud: Is this customer who they claim to be?

Any business that processes payments online opens itself up to fraudsters, who use stolen payment information to buy physical or digital goods or test stolen credit card information. The business bears the burden of fraud in a number of ways: they may lose an item to the fraudster, they have to refund the bank and credit card holder, and they’re stuck paying a chargeback fee. If the problem grows too large, banks might place the business in a chargeback monitoring program, with increased fees and the threat of losing access to certain issuers. Payment fraud is damaging to a business’ bottom line, and can also have knock-on effects to the brand’s integrity.

Account abuse: Does this “user” have legitimate intentions?

User growth is becoming an increasingly important indicator of an online platform’s sustainability – and may even be valued above revenue. But any website that permits signups is vulnerable to bad actors creating fake accounts with malicious intentions – which may include money laundering, theft of confidential information, account takeover, credit card fraud, phishing, or spam. Fake signups threaten the integrity of these sites, devalue their user base, and drive loyal users from the platform. Essentially, fake users are a continuing liability.

Content abuse: Will this person interact with the community safely?

The primary trust concern of social networks, marketplaces, dating sites, crowdfunding sites, and other online platforms that allow user-generated content is keeping the community safe and free of abuse. When used as intended, every new listing, profile, message, or campaign is an opportunity for the platform to thrive and engagement to grow. When misused, however, they provide an opportunity for a malicious user to annoy, scam, or cause harm to legitimate users – and, by extension, the site's brand. For these online businesses, the question of whether a user is likely to create malicious content may come up at multiple points in the user's journey – from the moment they create an account to when they fill out their profile to when they create their first listing, or respond to someone else's.

Promo abuse: Is this user gaming the reward system?

Online businesses are increasingly offering promotional credits – awarded either for joining or referring a friend – to quickly grow their user base. However, fraudsters are intentionally gaming the terms of these coupons or referral codes for their own benefit by using multiple email addresses and fake accounts. As a result, businesses are losing revenue and wasting marketing spend, while not actually acquiring new customers. What may start as a small, nagging expense can soon turn into a larger problem that puts a real dent in your revenue.

A challenging landscape

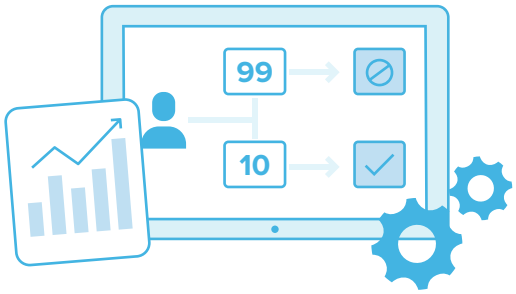
No company makes a trust decision in a vacuum. As online businesses scramble to respond to threats from multiple directions, they're also working within an increasingly competitive and technologically challenging environment.

More data, more complexity

Today, there are more devices and more channels sending an increasingly diverse set of data to companies, which makes it harder to piece together the story of who a user really is. Someone may create an account on an online marketplace using their desktop computer, confirm their email using their Apple watch, and make a purchase on their phone. They may

pay using a digital wallet or virtual currency. They may leave a seemingly endless trail of small interactions – profiles visited, messages sent – across your site. Suspicious behavior is often buried within streams of data.

Bottom line: To make the best trust decisions, you need to be able to quickly process and accurately analyze enormous data sets, working across devices and channels.



Globalization is growing

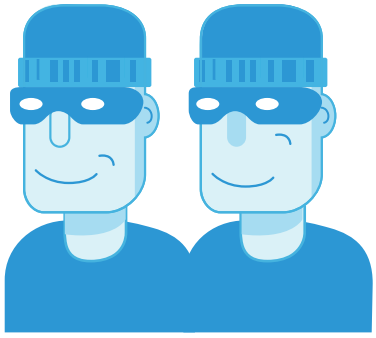
The advent of the internet means that any business can now take advantage of international expansion – and, as a result, cross-border commerce is booming. Shoppers are expected to spend $307 billion on cross-border e-commerce purchases by 2018, up from $105 billion in 2013, according to The Nielsen Company. Meanwhile, peer-to-peer marketplaces and communities make it possible for buyers, sellers, and users to transact and interact with each other – in real time – from any location in the world.

As businesses strive to take advantage of untapped markets, making smart trust decisions can become more challenging. Behavior that is trustworthy in one culture may not be in another – and vice versa. Rules, blacklists, and other traditional approaches to making trust decisions no longer work – and can even get in the way of your growth.

Bottom line: To make the best trust decisions, you need to understand the contextual significance of individual data points across geographies.

Online criminals are adapting quickly

For those with fraudulent aspirations, the path to profit is sadly within their reach. The huge data breaches of the recent past have flooded the dark web with financial and personal information. All of the hardware and software needed to commit fraud at scale are on sale, often for disturbingly low prices.



Today's online businesses are facing an increasingly sophisticated enemy that attacks,

responds, and changes tactics extremely quickly. Worse still, cybercriminals are increasingly targeting non-monetary information that makes it easier to commit account-level crimes.

Bottom line: To make the best trust decisions, you need the flexibility to adapt and evolve as cybercriminals continuously improve their tactics.

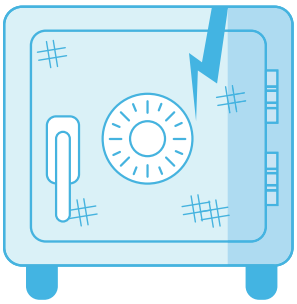
Real time is the new reality

Speed and user experience have become true competitive differentiators. One-click ordering, next-day delivery, and instant gratification are part of the new norm of customer expectations.

For some newer business models – like on-demand services and digital goods – there's no time to manually review orders before they're fulfilled. The ability to make an instant trust decision is more than a nice-to-have; it's a business requirement.

Bottom line: To make the best trust decisions, you need to gain actionable intelligence from all possible data inputs instantaneously, so you can act as quickly as possible.

The price of misplaced trust



So many small decisions are made each day, and each one comes with a cost. If you wrongly trust someone – in other words, mistakenly allow a bad actor to buy something, or create an account, or post content – the repercussions to your business can be devastating.

There's the obvious financial damage that prompts retailers and e-commerce sites to bulk up their risk departments, with more than $7.2 billion projected to be lost to card-not-present fraud by 2020. This is what may immediately come to mind when someone says "fraud": a criminal with a stolen credit card, trying his luck to buy a stereo system online that he can resell down the street.

Although difficult to assign a dollar sign to, the effects of a negative user experience can be just as damaging as a direct hit to your bottom line. Spam, fake content, phony listings, and unwanted messages on an online platform function like sidewalk litter and graffiti outside a shop: small but observable acts of bad behavior that spur even more bad behavior and sow distrust throughout the community.

Users take note of less-than-stellar experiences. When a user has their credit card misused or is scammed on your site, they don't just blame the "bad guy" – your company is also on the hook. Plus, they probably aren't going to just keep that bad experience to themselves;

they'll share it with friends and family, or even on social media. There may even be legal and compliance issues to deal with, if a fraudster is abusing your terms of service.

The price of distrust: are you paying the trust tax?

While misplaced trust is clearly a threat to the financial and brand health of today's online businesses, it's important to remember that's only one side of the coin. What happens when a business extends too much distrust? An often overlooked cost of making bad trust decisions is the price that businesses pay when they can't confidently trust their legitimate users. We call this cost the "trust tax." While not every business tracks this metric, every business should. It's the real growth killer.

Remember airport security, how the malicious actions of a small number create a less-than-ideal experience for the majority? Similarly, a business that is afraid of fraud and abuse, or is not equipped with the right tools to measure risk, may be overzealous in blocking or rejecting suspicious users. Or they may add friction to their signup or buying process to keep bad users out – an approach which results in less fraud, but also fewer signups or sales.

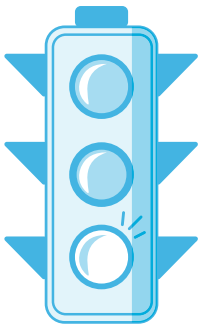
So, what does a business miss out on when they block a good user? First, it means you miss out on revenue. Some $118 billion in legitimate orders were incorrectly rejected in 2014, according to Javelin Research. And businesses may also lose future sales; false declines – also called "customer insult" (for good reason) – alienate shoppers. One-quarter of people who'd had a purchase declined said they didn't shop as much with that merchant afterwards, while 32% stopped shopping there altogether.

But you don't have to reject someone outright to feel the pain of misplaced distrust. Just as damaging is the effect of adding friction to the user experience. How many users would have finished signing up for an account if they didn't have to scour their inbox to confirm their email address? How many people would successfully create a classified listing if they didn't have to fill out a CAPTCHA that's really hard to see on a tiny mobile screen? How many shoppers would have completed their purchase if they didn't have to track down their physical credit card to verify the CVV code?

The saying goes, "you only have one shot at a first impression." Well online, you only have one opportunity to create a positive user experience. If that experience falls short, you probably won't get another chance. The trust tax is the price you pay for standing in the way of a legitimate user doing what they want to do quickly and effortlessly.

Online businesses who understand the power of trust, and who are truly invested in creating an outstanding user experience, are already introducing ways to "reward" legitimate users by smoothing their way through checkout or signup or posting – and are reaping their own rewards in the form of increased revenue, growth, engagement, and brand loyalty. While the risks of misplaced trust may seem huge, the benefits of being generous with trust – to the right people – are even larger.

A better way to make trust decisions



As you can see, answering the deceptively simple question of "Can I trust this user?" requires a fairly sophisticated approach. But what does that approach look like?

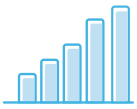
Making sense of fraud and abuse signals at scale

As a consumer, there are lots of signals that demonstrate whether a website or app is trustworthy. A retail site may include the Better Business Bureau seal, an app may sport thousands of positive reviews in the Apple Store, and an online community may surface social proof at signup, showing you that it already boasts some of your friends as active users.

From an online business' perspective, making the decision to trust or not to trust a user is far more complicated. On any given day, an individual may visit (and make trust decisions about) a dozen different sites, max. But an online business may contend with making trust decisions about thousands or even millions of visitors on that same day. And each of the billions of human beings on earth don't traverse the web with a built-in "trust score" that would tell you – at a glance – whether you should allow that person to buy something, create an account, or post content.

However, online businesses do have a variety of signals at their disposal, which can be grouped into three main buckets: identity, behavior, and network.

› **Identity**. This is the fundamental question for any trusted relationship. Who is this person? Do I know they're who they claim to be? Online, this takes the form of things like device ID, email address, shipping address, social media profiles.



› **Behavior**. How are they acting? Are they behaving responsibly and considerately? Living up to their promises? Online businesses could look at how a user is interacting with the site or app, what they're clicking on, how many purchases they're making within a short time frame, etc.

› **Network**. This is where you rely on others to double-check your own observations – or even give you a proactive heads up. Who else in your network has seen this person? What have they observed? Online, this signal could come from pooled data or information across a number of web properties.

There are thousands of small yet important signals available to help business make good trust decisions. The real challenge is bringing all of them together, making sense of them, and accurately assessing risk...all at the incredibly fast speed that online businesses need to move to stay competitive.

A flexible, adaptable platform

The good news? The technology to help businesses make the best trust decisions exists today. Machine learning processes enormous and diverse data sets in real time, as transactions and interactions are actually happening, largely taking the guesswork and loopholes out of catching deceptive and malicious users.

Machine learning adapts and learns as it ingests and analyzes more data, making it ideal for adapting to a rapidly changing threat environment.

By leveraging machine learning to get ahead of new methods of fraud and abuse, online businesses can instantly identify known and unknown users, and parse out real and bogus Best of all, machine learning is flexible enough to support a full range of trust decisions, so you can address multiple threats to your business while also delivering an amazing experience to legitimate users across multiple touchpoints. No one wants to feel like they're going through airport security when they're just trying to buy something, post content, redeem a promo, or sign up for an account. And no online business needs to settle for delivering that kind of experience. The opportunity to supercharge your business' growth through trust is within your reach.

Contact

scientists@siftscience.com
www.siftscience.com