Leading the Digital Trust & Safety Transformation

Unlock new revenue without risk

Contents

A call for change

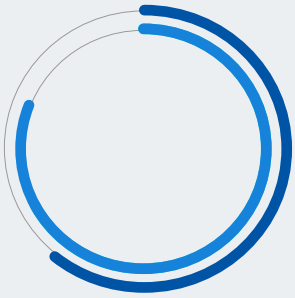
Blockbuster. Toys "R" Us. Kodak. Sears. What do these once market-leading brand names have in common? They didn't evolve to meet customer demands, and they paid the price. Today's businesses face the same challenge, every day.

Attracting, delighting, and retaining customers is at the heart of winning market leadership. The key to beating your competition is to meet — or, better yet, exceed — customers' incredibly high expectations. So the onus is on you to roll out new features and experiment with new revenue models, products, and capabilities that grow revenue. But the onus is also on you to manage this growth safely and securely.

In an effort to further understand how businesses are balancing fraud prevention and growth, we surveyed 500 employees responsible for fighting fraud.* The findings were clear: **staying ahead of fraud is more difficult than ever, meeting customer demands is more complicated, and the way businesses have been fighting fraud no longer works.**

The traditional mindset towards managing risk has focused almost exclusively on preventing loss. The organizational structures, processes, and tools that accompany legacy approaches sprang from a single goal: risk mitigation. They focus all their attention on finding and eliminating the <1% of users who are bad, while losing sight of the 99%+ who are legitimate. Little or no emphasis is placed on maintaining a great customer experience, increasing user engagement, or enabling revenue growth.

Just look at the shortcomings of legacy fraud prevention: rules-based systems and manual review teams. Not only are these approaches reactive (more "fraud mitigation" than "fraud prevention"), they also don't scale. Whether you are a mid-sized organization growing into an enterprise-scale company or a brick-and-mortar retailer in the midst of digital transformation, your tenuous grasp on "staying ahead" can feel like it's always slipping away.



77%

of online businesses prioritize delivering a frictionless experience

YET

58%

say fraud prevention blocks this goal

Source: Sift Digital Trust & Safety Survey, 2019

** The Sift Digital Trust & Safety Survey was carried out by Berg Research, in independent research firm. It surveyed 500 professionals at companies of 500+ employees across North America with responsibilities related to fraud, risk, mobile or e-commerce operations, and strategy.*

Legacy rules fall short

60% of companies using rules for fraud prevention say rules **BLOCK** legitimate customers

60% say rules **DO NOT** allow them to deliver a frictionless experience

45% say rules **DO NOT** prevent fraud effectively

44% say rules **ARE NOT** efficient for the team

Source: Sift Digital Trust & Safety Survey, 2019

Using a legacy approach to manage risk and enable growth is no longer effective. You need a fresh approach that provides agility and flexibility. One that gives you the freedom to grow, innovate, introduce new products, features, and business models — without increased risk. You need **Digital Trust & Safety.**

You can't wait to evolve. If you wait, you will lose out in market share and in customers. You will be left behind as your competitors seize new revenue opportunities from your grasp. The time to change is now. On the following pages, we show you why and how.

"We built our cross-functional Trust & Safety organization to proactively detect and prevent a wide range of abuses that could negatively affect our members.

Our teams work hard to drive a positive member experience, and that means creating a trusted environment to connect safely. But operationalizing Trust & Safety is a group effort and we work collaboratively with teams across the company to ensure we're building products with a members-first approach and staying ahead of new fraud trends."

Paul Rockwell
Head of Trust and Safety at LinkedIn

Survey: Rising fraud, rising demands

When fighting fraud, the stakes are high. You navigate a continuous balancing act between protecting your business and users from harm, and enabling revenue growth. Focus too much on preventing fraud and you risk stunting opportunities for moving into new markets, introducing new features, and releasing new products. But neglecting fraud can have a devastating impact on your bottom line.

As our survey results show, balancing these competing demands has never been more complex.

New opportunities, new challenges

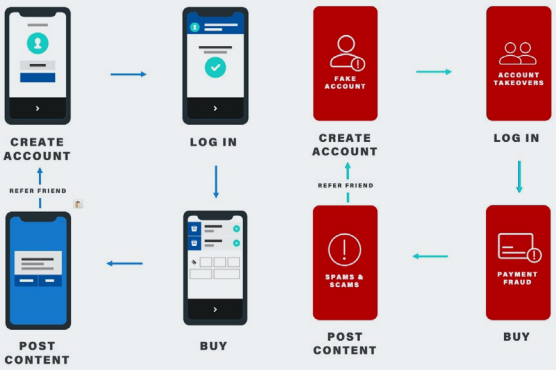
The description of "online fraud" used to be straightforward: using a stolen credit card to make a purchase. But *Sift Digital Trust & Safety Survey* respondents report that criminals have definitively broadened their tactics beyond stolen credit cards, taking advantage of online businesses and their users in new ways.

While two-thirds **(64%) of respondents face payment fraud**, an equal amount **(63%) are battling fake accounts.** Meanwhile, **42% deal with account takeover,** and **55% are fighting fake or spammy content**.

This broader spectrum of fraud risk arises as businesses add more features and capabilities to increase user adoption and engagement. One-click checkout, peer-to-peer marketplaces, digital goods, customer reviews, and referral programs are popular among consumers. But criminals are adapting their techniques to exploit those very features, making it harder to keep pace with evolving attacks.

The spectrum of online fraud risk

For every revenue-generating call to action on a website, there is a corresponding way for fraudsters to exploit that opportunity.



CALL TO ACTION	FRAUD VECTOR
Create account	Fake accounts
Log in	Account takeover
Buy now	Payment fraud
Create listing / posting	Scams
Post comment / review	Scams, spam, toxicity
Refer a friend	Fake accounts

Going hand in hand with these new business models are consumers' relentlessly rising expectations for speed, convenience, and seamless experience across all channels.

For risk teams, these new expectations, features, and business models are much harder to secure.

Speedy, convenient... and fraudulent?

Consumers are hungry for on-demand services, digital goods, peer-to-peer marketplaces, and one-tap checkout. But businesses that adopt these business models, products, and features face unique risks:

- **Fewer data points to rely on for building a risk profile**
- **Little to no time to manually review orders before they're fulfilled**
- **Low transaction which attracts card testing**
- **Behavior of risky users that may appear similar to legitimate users**
- **Difficulties of policing user-generated content**

Staying ahead of fraudsters is harder than ever

Respondents also report that criminals are getting better at anticipating new protection tactics and uncovering vulnerabilities. Nearly two-thirds **(64%) of survey respondents said they haven't fully achieved the goal of staying ahead of fraud patterns**.

> "Coming up with ways to counter new fraud techniques is our biggest challenge. It's harder and harder to keep up."

C-level executive in the Finance industry

To try and keep up, businesses are buying more tools to supplement the shortcomings of their existing fraud stack, and adding more employees. But does increased spending yield positive results?

Business as usual isn't working

69%
spent more on fraud this year

BUT

65%
say fraud continues to rise

So why do 95% plan to add more tools or people to manage fraud in the next 12 months?

Clearly, the status quo is not working. Companies are investing in the same methodologies they always have, and expecting a different result. Meanwhile, the world is changing around them: fraudsters are getting more sophisticated, and users' expectations are getting higher.

Digital Trust & Safety: A new paradigm for balancing growth and risk

Digital Trust & Safety is an approach that strategically aligns risk and revenue decisions, supported by processes and technology. With Digital Trust & Safety, you can seize new revenue opportunities and increase customer satisfaction, without risk.

The 4 qualities of a Digital Trust & Safety organization

Evolving from legacy approaches, organizational structure, and tools requires a change in mindset. Digital Trust & Safety is about more than adding a new tool or procedural step; it's about remodeling business strategies for the challenges and opportunities of the digital world. This framework encompasses changes in mindset, processes, and technologies.

Balances growth with security

MINDSET: Prioritizes providing an outstanding experience equally to protecting the business

PROCESSES: Risk team actively supports revenue growth by enabling new products, features, and regions to launch faster and more smoothly

TECHNOLOGY: Leverages dynamic friction to create an appropriate experience for each user, based on risk

Cross-functionally aligned

MINDSET: Sets shared goals that encompass both risk mitigation and revenue growth

PROCESSES: Risk/fraud teams are stakeholders in growth/product decisions, and vice versa

TECHNOLOGY: Shares fraud, product, and marketing data across teams, for the benefit of all

Holistic

MINDSET: Focuses on entire customer journey and experience, rather than discrete actions and events

PROCESSES: One centralized or cross-functional group manages the strategy and prevention of all fraud and abuse vectors

TECHNOLOGY: Incorporates learnings from across the entire user lifecycle, not just the point of transaction

Forward-thinking

MINDSET: Creates a strategy and technology stack that is future-proofed, not reactive

PROCESSES: Relies on automation to scale risk processes successfully

TECHNOLOGY: Invests in technology that learns and adapts to new fraud patterns automatically

Benefits of Digital Trust & Safety

MORE REVENUE — With a rise in good orders approved automatically, you increase your top-line growth.

NEW OPPORTUNITIES — Aligning goals gives you the ability to introduce new products and move into fresh markets without risk.

INCREASED USER SATISFACTION — With fewer purchase roadblocks and a more personalized checkout experience, users have a better experience on your platform.

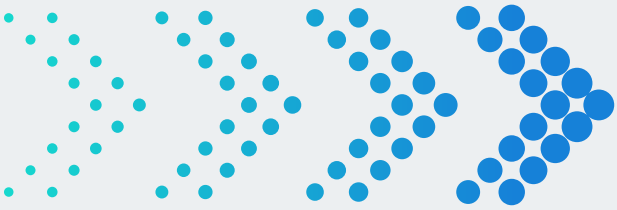
ABILITY TO SCALE — Bolstered by technology that constantly learns and adapts to evolving fraud patterns, you can automate processes that allow you to grow your customer base and bottom line.

How to evolve to Digital Trust & Safety

Depending on where you are in your fraud prevention or digital transformation journey, you may require different steps to evolve to a Digital Trust & Safety approach. You must make changes to your mindset, organizational structure, processes, and technology.

Mindset

Driver of change: Company executives



FROM...	TO...
Minimizing risk and protecting the bottom line	Prioritizing outstanding customer experiences and top-line growth, as well as risk mitigation

Risk prevention is at the core of a traditional e-commerce mindset. In fact, our survey found that 86% of executives are involved or very involved in fraud prevention. This reflects a C-level understanding of the importance of protecting the bottom line.

However, all too often this focus is not aligned with company initiatives that support growth. Nearly three-quarters **(73%) of businesses said they are not able to fully achieve their goal of launching new products without increasing risk**. And 71% said the same about moving into new markets. Furthermore, more than half **(57%) of respondents admitted that revenue-driving goals and fraud prevention goals are not fully aligned**.

To win in the digital economy, you need to equally prioritize growth opportunities and the measures that support them. Because of the bottom-line impact of fraud loss, organizations over-index on security checks and measures to keep bad actors out, at the expense of good users' experience.

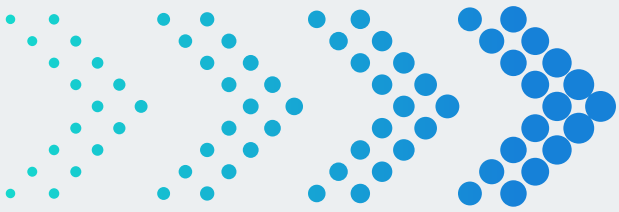
Shifting from a risk mindset to a growth mindset requires buy-in and evangelism at the executive level. When these growth-positive measures are built into a company's fabric, it allows them to add revenue and increase user engagement, without sacrificing safety.

ACTION ITEMS

- ☐ **Define goals for what Digital Trust & Safety will achieve, which roll up to other company-level initiatives**
- ☐ **Assess how Digital Trust & Safety relates to other company efforts, such as digital transformation**
- ☐ **Share the vision and how it benefits both end users and the company**

Organizational structure

Driver of change: Company executives



FROM...	TO...
Siloed departments, with misaligned goals, not sharing tools, data, or best practices	A cross-functional or centralized team pooling information and learnings

Currently, only 4% of organizations have fraud departments reporting up into Trust & Safety, according to the 2018 CNP Fraud Operations Study. Instead, the most common reporting structures are Finance (32%), Operations (15%), and Customer Service (11%).

When reporting into siloed areas, organizations run the risk of prioritizing only what matters to that department. For example, the Finance team may be overly focused on the bottom line, and may not allocate budget to types of fraud where the dollar impact isn't as visible, like content abuse. And Customer Service may be setting goals primarily around reducing user complaints, while deprioritizing other signals of fraud.

Siloed goals are the reason that there is often tension between risk teams and those that are focused on growth or marketing. Risk teams may block suspicious users (which can interfere with growth in monthly active users) and block or refund transactions (getting in the way or revenue goals). They may also advocate for using verification steps like CAPTCHA, 3D Secure, or two-factor authentication — which can lead to lower signups and sales. Conversely, growth and product teams may want to launch features the fraud team deems risky.

Trust and safety teams are by nature cross-functional, and operate with aligned goals. Team members may come from Product, Customer Support, Data Science, Engineering, Growth, and more.

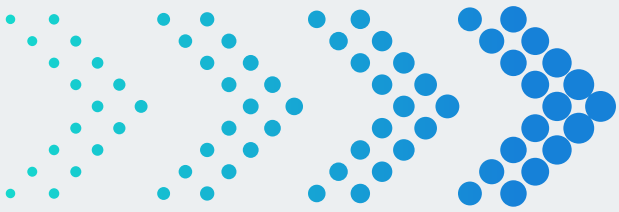
The key is to ensure that all viewpoints are heard, risks vs. rewards are weighed, and decisions are made as one team. Organizations that succeed are those who have aligned incentives, that take into account both risk and revenue — ensuring that the first is minimized, while the second is maximized.

ACTION ITEMS

- ☐ **Create a framework for achieving Digital Trust & Safety goals and assign owners**
- ☐ **Create guiding principles on how to measure risk vs. reward**
- ☐ **Build cross-functional lines of communication**
- ☐ **Incentivize groups to collaborate on joint goals**

Processes

Driver of change: Fraud Manager / Director



FROM...	TO...
Risk teams getting involved in product development post-launch	Collaborating cross functionally to build security into launches, for the collective benefit of users and the company

As stewards for company safety, fraud teams are called upon to "get involved" with a product launch and ensure it goes smoothly. But all too often, this means bringing them in to check a box late in the process. Nearly two-thirds **(64%) of survey respondents say that fraud teams are not fully involved in product development**. Risk teams are not actively involved in strategic conversations. Moreover, they typically only have access to siloed data from their own team.

With a Digital Trust & Safety mindset, the risk team is a cross-functional collaborator in launches from the start. And everyone pulls from the same central repository of data, which includes data on how users interact on the platform, what pages they have viewed, time spent on each page, what products they've bought, email correspondence, etc.

This aligned way of working has multiple benefits:

- **Products are better, since they are built with both protection and growth in mind**
- **Launches move faster and more smoothly**
- **Conversations happen earlier, so there are no surprises at the end**
- **The need for reactive post-launch cleanups is eliminated**

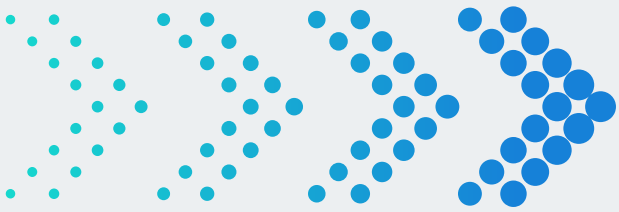
Having access to the right data will also enable aligned decisions around risk vs. growth. In other words, how are growth initiatives affected by risk policies, and vice-versa? This will help teams come together to strike the right balance.

ACTION ITEMS

- ☐ **Gather data from risk, marketing, and business insights teams to store in a central repository**
- ☐ **Align on how to balance risk and growth from an operational standpoint**
- ☐ **Identify gaps to close, where your system can be abused**
- ☐ **Identify what security checks are in place that don't need to be**

Technology

Driver of change: Fraud Manager / Director or technical lead



FROM...	TO...
Reactive, inflexible rules based on data from the point of transaction	Adaptive machine learning leveraging data from the entire user journey, with flexibility to customize friction

Traditional fraud prevention tools arose from the need to block bad actors and reduce loss. With these tools, you react to observed fraud trends with rules. The result? Fraudsters adapt and outmaneuver rules, while good customers who inadvertently get caught in the net leave your site for one that provides a better experience. This creates a cycle where you're spending more time creating rules to stay ahead of fraud, while simultaneously driving away good customers with every rule you create. In our survey, **60% of companies using rules for fraud prevention said that rules block legitimate customers**.

With machine learning, you don't need to spend time trying to spot fraud trends. Instead, you can strategically think about what kinds of experiences you want to deliver to your users. Machine learning adapts in real time to assess risk and routes users to the appropriate experience based on that risk. This approach is not about blocking bad users; it's about tailoring the user journey.

Proactively identifying risk is only possible when you capitalize on the wealth of insights from across the customer journey, including behavioral data such as pages visited, time on page, keystrokes, referral source, and more. As fraud becomes more sophisticated, these are the signals that help you tell good users from bad users. Machine learning detects these patterns and adapts in real time — enabling you to deliver tailored user journeys even as user behavior changes.

In *Online Payment Fraud: Emerging Threats, Segment Analysis & Market Forecasts 2018-2023,* Juniper Research highlighted the missed opportunity of focusing solely on transaction data, and encouraged businesses to incorporate behavioral data as well.

> "A layered solution naturally helps directly preventing fraud, but it also offers major gains in terms of recovering potentially lost revenue through false positives."

Stefan Sorrell, Juniper Research

ACTION ITEMS

- ☐ **Understand how machine learning is different than other fraud prevention approaches**
- ☐ **Identify what user data is stored that could be used for machine learning**
- ☐ **Determine how machine learning layers in with rules, reporting and your console**

The time for Digital Trust & Safety is now

As traditional retailers and digital native e-commerce companies alike face the competitive pressures of the digital world, change is no longer an option — it's a competitive necessity. Organizations' ability to adapt to an increasing range of threats, as well as meeting the rising expectations of today's consumers, will separate winners from losers.

As leaders, you need to challenge comfortable ideas, learn about the new tools and processes that will guide your company forward, drive core processes, and embrace innovation. You need to change mindsets across your entire organization. As the saying goes, the only constant is change. Those who do not adapt will be left behind.

See Digital Trust & Safety in action

 |