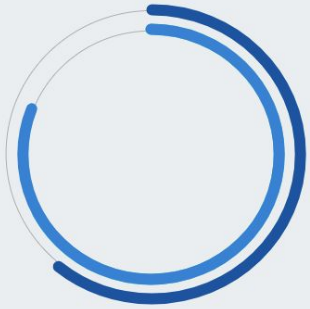
Digital Trust & Safety: Aligning Security and Growth Strategies

Introduction: 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 competition is to meet – or, better yet, exceed – customers' incredibly high expectations. So the onus is on businesses to roll out new features and experiment with new revenue models, products, and capabilities that grow revenue. But the onus is also on them to manage this growth safely and securely.

In an effort to further understand how businesses are balancing fraud prevention and growth, Sift 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 used to fight fraud no longer works.**



77%

of online businesses prioritize delivering a frictionless experience

YET

58%

say fraud prevention blocks this goal

Organizations need to move beyond traditional mindsets

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 focused all their attention on finding and eliminating <1% of their users who were bad, while losing sight of the 99%+ who are legitimate. Little or no emphasis was 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 organizations are mid-sized growing into an enterprise-scale company or a brick-and-mortar retailer in the midst of digital transformation, “staying ahead” can feel like it’s always slipping away.

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

Rising fraud, rising demands

The description of “online fraud” used to be straight forward: using a stolen credit card to make a purchase. But now criminals have definitively broadened their tactics beyond stolen credit cards, taking advantage of online businesses and their users in new ways.

This broader spectrum of fraud risk arises as businesses add more features and capabilities to increase user adoption and engagement.

63%
Battle fake accounts

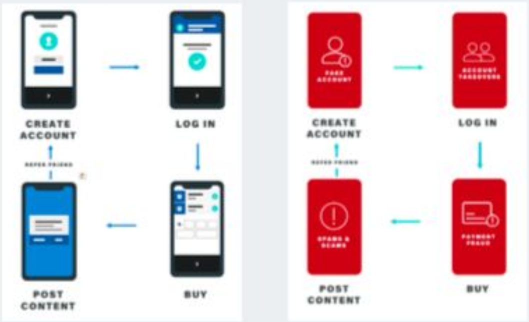
42%
Deal with account takeover (ATO)

64%
Face payment fraud

55%
Fight fake or spammy content

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

Rising fraud, rising demands

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 amounts attract rampant card testing**
- **Behavior of risky users may appear similar to legitimate users**
- **Difficulties of policing user-generated content**

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.

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.

Staying ahead of fraud is harder than ever

Criminals are getting better at anticipating new protection tactics and uncovering vulnerabilities.

In an attempt to keep up, businesses are responding by spending money on more tools to supplement the shortcomings of their existing fraud stack, and adding more employees to address problems.

Clearly, the status quo is not working. Companies are investing in and applying 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.

64%

HAVE NOT fully achieved the goal of **STAYING AHEAD OF FRAUD PATTERNS**

65%

are seeing **MORE FRAUD HIT THEIR SITES**

69%

SPENT MORE ON FRAUD THIS YEAR than in the previous year

58%

hired more **FRAUD-FOCUSED EMPLOYEES**

95%

plan to **ADD MORE TOOLS OR HIRE MORE PEOPLE** to manage fraud over the next 12 months

Misalignment across the organization

All too often departments across the organization are not aligned with company initiatives that support growth. This reflects a C-level understanding of the importance of protecting the bottom line.

> “Keeping up with new fraud techniques and coming up with new ways to counter them is our biggest challenge. Fraud technology is constantly changing, and it’s becoming harder and harder to keep up.”

C-level executive in the Finance industry

86%

of executives are **INVOLVED OR VERY INVOLVED** in fraud prevention.

57%

admitted that revenue-driving goals and fraud prevention goals are **NOT FULLY ALIGNED**.

73%

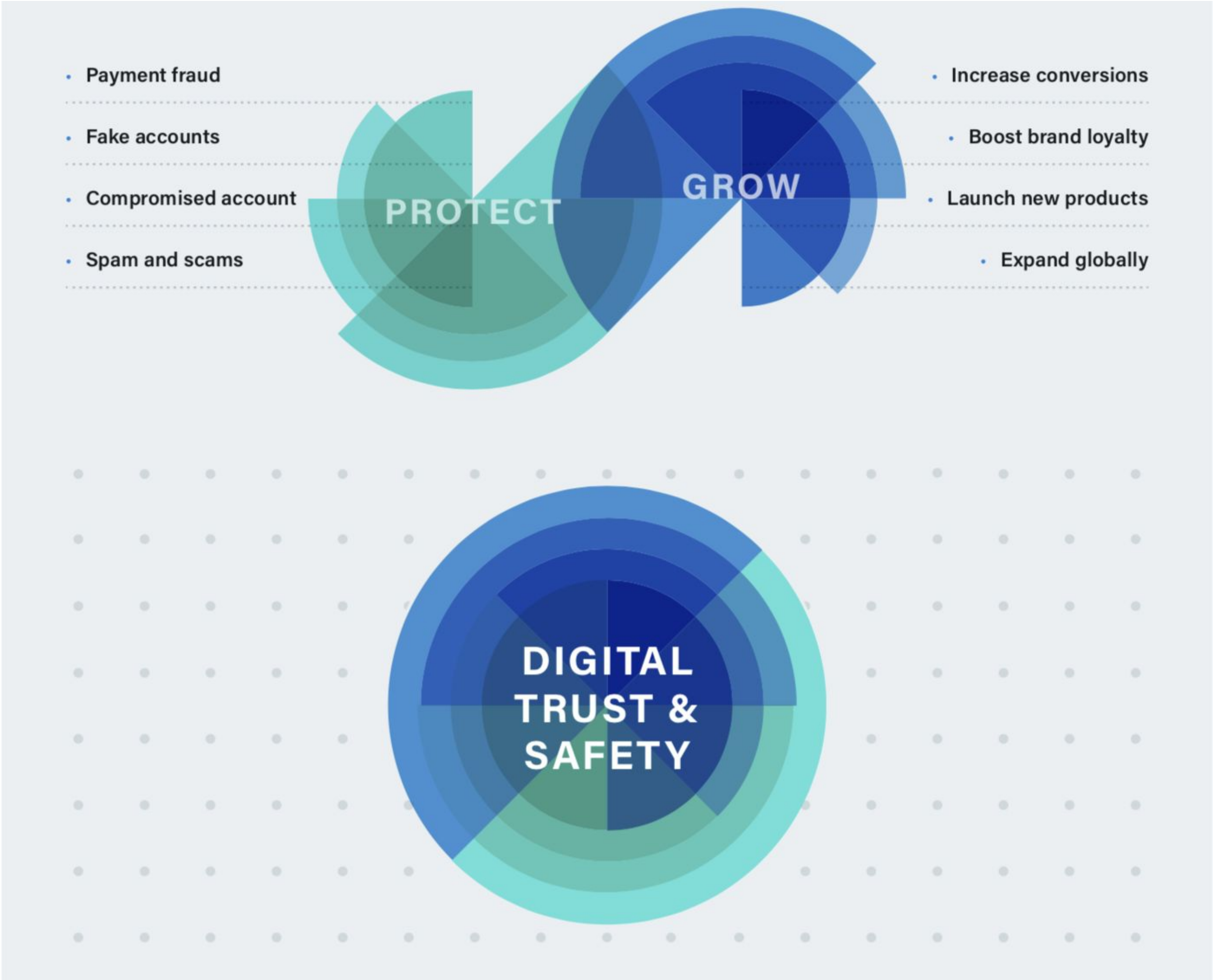
of businesses said they are **NOT ABLE TO FULLY ACHIEVE THEIR GOAL** of launching new products without increasing risk.

71%

SAID THE SAME about moving into new markets.

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.



- Payment fraud
- Fake accounts
- Compromised account
- Spam and scams

- Increase conversions
- Boost brand loyalty
- Launch new products
- Expand globally

The four 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: Providing an outstanding customer experience is equally important as 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: Focused 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

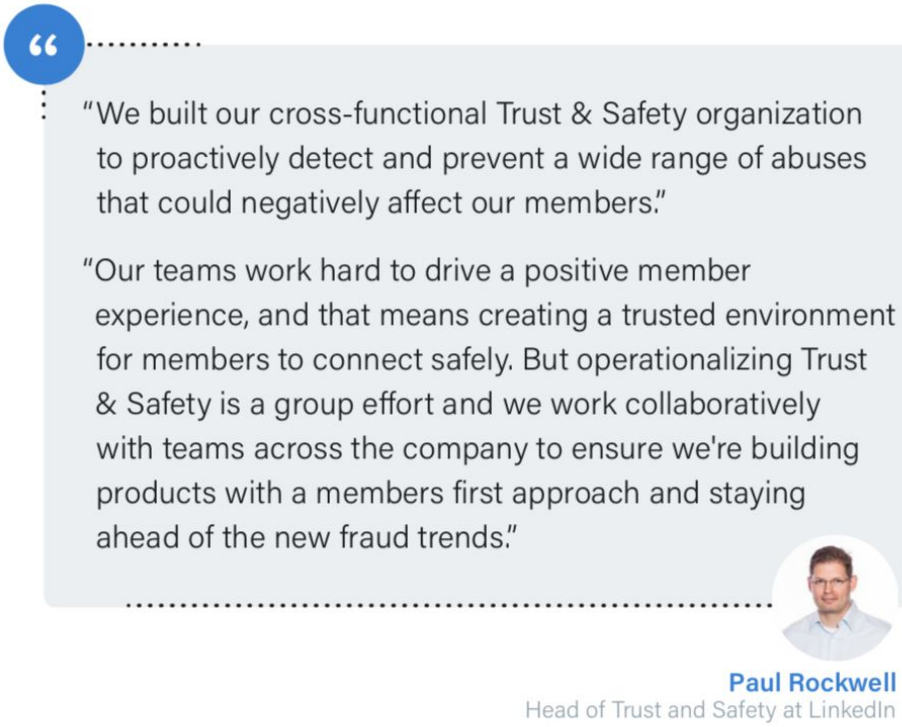
PROCESSES: Relies on automation to scale risk processes successfully

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

The time for Digital Trust & Safety is now

As traditional retailers and digital native e-commerce companies alike face the increasing competition 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 ever-increasing expectations of today's consumers, will separate winners from losers.



"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 for members 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 the new fraud trends."

Paul Rockwell
Head of Trust and Safety at LinkedIn

Survey Methodology
The Digital Trust & Safety: Aligning Security and Growth Strategies survey was commissioned by Sift and fielded by Berg Research, an independent research firm. The responses were generated from a survey of 500 professionals across North America with responsibilities related to fraud, risk, mobile or ecommerce operations and strategy. These professionals represent companies with 500+ employees throughout North America and across online retail industries, such as travel, hospitality, ecommerce, etc.