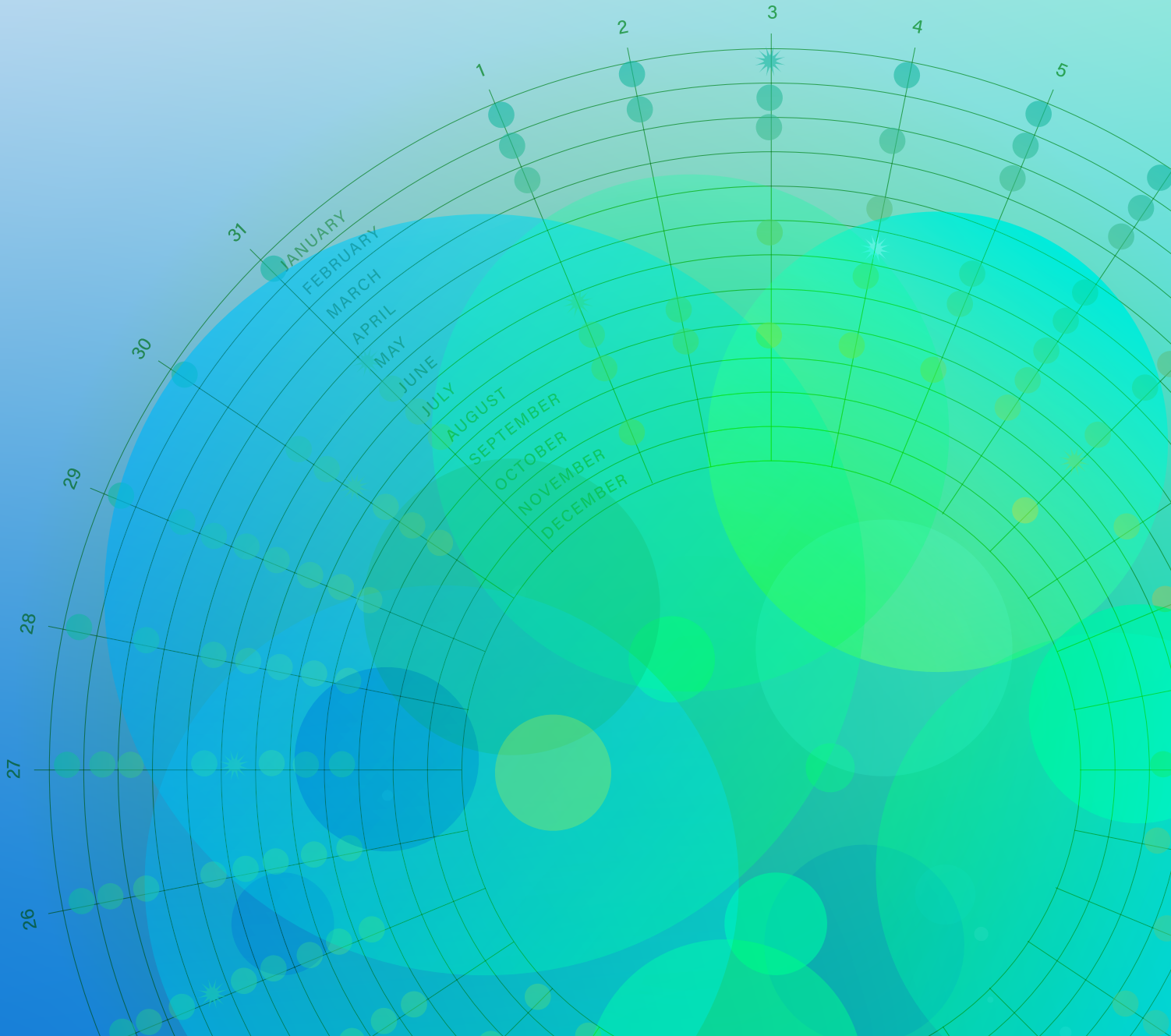
sift

Q1 2022 DIGITAL TRUST & SAFETY INDEX

Outsmarting payment fraud in the age of automation



Contents

PAYMENT ABUSE IN THE FRAUD ECONOMY

Growth-fueled Risk and Moving Targets

Payment fraud decapitates business growth. But before a company even begins to realize its potential, fraudsters hellbent on financial theft can attack vulnerabilities across on-site customer journeys, and across the internet, stealing data and funds—putting online merchants at risk long before a login, transfer, or transaction even takes place.

1	2	3	4	5
+121% Fintech	+34% Travel and hospitality	+29% Digital Goods/ Services	+24% Marketplaces	+6.3% On-demand

% increase YoY in order volumes by industry, 2020-2021.

Fraudsters have plenty of motive to snatch revenue when the probability of a payout is so high: last year, consumers spent $871 billion online with U.S. merchants alone, up 14.2% year-over-year. Between 2020-2021, average daily transaction volumes across Sift's global merchant network rose in every industry, with the biggest surge in fintech at **121%** growth YoY.

Order volumes shot up by about **24%** in marketplaces, and **34%** in travel & hospitality, signaling new fluctuations in demand for markets hit hard by the pandemic. And while volumes rose less dramatically in digital goods & services, on-demand, and retail, fraudsters follow growth and spend wherever it shows up—and the pool of potential victims gets larger by the day.

Nearly half of consumers surveyed by Sift* (**49%**) have fallen victim to payment fraud over the past 1-3 years, with **41%** of those in the last year. Of those victims, **77%** had unauthorized purchases made using payment information the consumer had stored on a website or app.

In the Fraud Economy, cybercriminals leverage sophisticated, automated, and distributed strategies across different merchants and verticals simultaneously, committing account takeover (ATO), financial fraud, and multi-tiered scams at inhuman speed and scale. Attempted payment fraud jumped **23% YoY** across the entire Sift network in 2021, fueled in large part by organized fraud rings launching bot-backed assaults against businesses of every size.

The increased complexity of online abuse changes the goalpost for fraud prevention. Instead of solving for individual fraud vectors, relying on reactive responses, or expecting fraudsters to move on after a failed hit, trust and safety teams must proactively and universally eliminate opportunities for attack, with consideration for market-specific priorities and evolving consumer expectations.

of consumers have recently fallen victim to payment fraud.

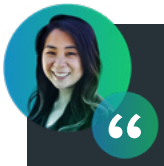
On behalf of Sift, Researchscape International polled 1,003 adults (aged 18+) across the United States via online survey in January 2022.

2020-2021

Fraud Rates and Trends by Vertical

Businesses in every industry suffer from blindspots around fraud prevention. These include incomplete security strategies that neglect hidden risks, or that stunt growth with unnecessary friction. Many merchants lack visibility into false positives and born-bad accounts, causing them to treat every user and transaction the same way. This deficient oversight into fraud's true impact is expensive: between 56%-74% of consumers would stop engaging with a brand due to fraud.

Fraud-fueled brand abandonment becomes a massive threat to growth when over half of self-reported payment abuse victims (**60%**) said they've experienced financial fraud more than once, and **25%** are "very" or "extremely" concerned about it happening again. Piling on to the problem, only **21%** of these victims were notified of suspicious activity by the merchant—the rest found out on their own, or via their card issuer—suggesting that limited protections are being put in place by businesses to detect and mitigate fraud.



JANE LEE, *Sift Trust and Safety Architect*

People likely feel most at risk when using financial services sites not because they're inherently insecure, but because it's where they keep their money. Consumers are going to equate a merchant's risk with how much they think, or know, they have to lose—whether it's loyalty points or their life savings.

One-third of payment fraud victims (**33%**) pointed to financial services sites as highest-risk, and they're right to be concerned: on the back of **121%** YoY growth in transaction volumes, payment fraud attack rates ballooned **70%** across finserv—the highest 2020-2021 increase of all parent verticals in Sift's network—hitting key subverticals especially hard.

Digital wallets saw a painful **200%** surge in payment fraud attacks, while PSPs and crypto exchanges saw attempted payment fraud inflate by **169%** and **140%**, respectively.

Fintech Breakdown: Fraudsters target digital wallets, crypto, PSPs

Most fintech providers saw an uptick in attempted payment fraud between 2020-2021, indicating that fraudsters are focused on areas with rocketing growth and popularity, like alternative payments and decentralized finances.

*Calculated based on the YoY fraud rates of the PSPs' merchant customers.

increase in YoY attempted payment fraud across Sift's global network, 2020-2021.

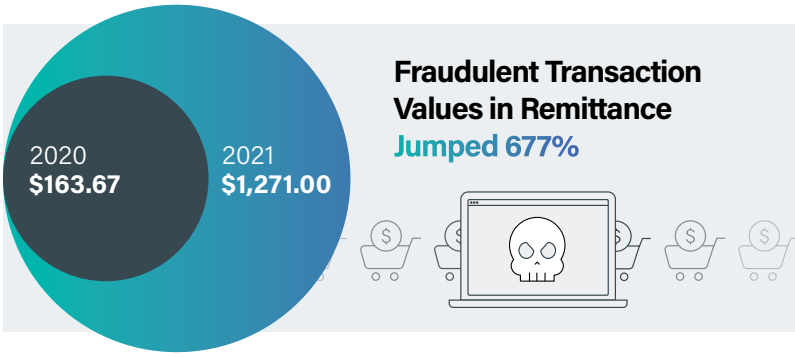
Rising fraud in the buy now, pay later (BNPL) space is another snowballing concern for merchants who offer point-of-sale loan options. The value of attempted fraudulent BNPL purchases rose by only **5%** in 2021, up to **$179.00** from **$170.55** in 2020. But the fraudsters who exploit these financial layaway programs aren't after big ticket items—rather, they're hacking into BNPL user accounts using stolen credentials that they've either purchased, phished, or otherwise hijacked. They can then use payment details, rewards balances, gift cards, and prepaid cards associated with those accounts to make purchases or trespass on other sites.

In addition to global increases in payment fraud attacks, certain subverticals saw average fraudulent order values spike dramatically. In remittance, they jumped by a gutting **677% YoY**, from **$163.67** in 2020 to **$1,271.00** in **2021**.

Where Consumers Have Encountered Payment Fraud

- **33%** Financial Services
- **29%** Retail
- **23%** Marketplaces
- **17%** Digital Goods & Services
- **8%** On-demand Services
- **8%** Travel/Hospitality

*Respondents were allowed to select multiple options.



Fraudulent transaction values also rose in crypto exchanges (**8%**), digital wallets (**9%**), and neo/challenger banks (**85%**).

Payment fraud rates went up in retail by a modest **12% YoY**, while average fraudulent order values more than doubled, increasing **2.5x YoY**. Rising payment fraud has unmatched power to destabilize retailers, which traditionally turn to friction in the user journey to stay secure—a common strategy that stops some fraud, but that turns away legitimate customers, too, upping a merchant's false-positive rate and costing them revenue. Retailers also often rely on manual review and verification, and while both are highly accurate, they're notoriously difficult, and expensive, to scale.

Rising Payment Fraud by Industry 2020-2021

All Network	23%
Fintech	69%
Digital Goods & Services	49%
On-demand Services	25%
Retail	12%

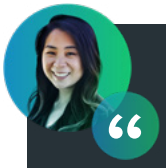
Merchants don't only pay for digital attacks in lost revenue, but in chargeback fees and lost lifetime value (LTV), too: **86% of consumers** would request a refund if they discovered their payment information had been used to make an unauthorized purchase, and 74% of consumers previously surveyed say they'd permanently stop engaging with a brand compromised by fraud. Furthermore, merchants are liable for interchange and misuse fees when it comes to card testing attacks and any resulting declined transactions.

Compounding the issue is that e-commerce companies typically guard proprietary consumer information that fraudsters want. **Two-thirds** (**66%**) of consumers store credit card or other payment details with online retailers, and **33%** save the credentials for their financial institutions in device-native password managers, placing the burden of protection heavily on merchants who offer these conveniences to users.

Changes in Fraudulent Transaction Values by Parent Industry

- 2020–2021
- 2021–2022

	2020–2021 Fraudulent transaction value	2021–2022 Fraudulent transaction value	YoY fraudulent order value
Travel & Hospitality	$332.22	$2,461.00	695%
Retail	$807.30	$2,779.00	244%
On-demand Services	$56.18	$127.85	128%
Marketplaces	$2,251.73	$3,129.00	39%



JANE LEE, *Sift Trust and Safety Architect*

> The brand damage done by payment fraud isn't just financial—it stains the merchant's reputation. When an unauthorized transaction shows up on a non-customer's bank statement because their payment information was stolen elsewhere, they will forever associate that merchant with fraud.

Between 2020-2021, fraud rates rose **25%** in on-demand services, largely due to a **24% YoY** spike across QSRs & food delivery. But fraudulent order values increased **128%** throughout the on-demand space, with the value of illegitimate purchase attempts in QSRs & food delivery up **59% YoY** and **276% YoY** across other on-demand providers. This illustrates more targeted, intentional attacks against merchants whose customers expect real-time and same-day access to goods and services.

Travel & hospitality were targeted by digital criminals making fewer, but bigger, bets: the average value of attempted fraudulent transactions in this vertical ballooned by **695%**, from **$332.22 in 2020** to **$2,641.00 in 2021**. On their own, online travel agencies & services were slammed by a **754%** surge in the average value of attempted fraudulent purchases, coming in at an average **$3,318.00** in 2021. Lodging & ticketing experienced significant jumps in fraudulent order values as well, up **250%** and **174%** respectively. And while the uptick in fraud across travel & hospitality was largely influenced by 2020 lockdowns giving way to renewed wanderlust in 2021, these individual, massive purchase attempts, in tandem with spiking transactions, also indicate more aggressive fraud throughout the industry.

With the frequency of fraud rising for large chunks of digital commerce, and no end in sight for the push to do more business online, businesses have to stop framing fraud as an account-level issue, a one-solution problem, or a necessary evil they must live with. Outmaneuvering sophisticated, tech-focused networks of fraudsters will take real-time response, accuracy, and adaptability; outsmarting them will require understanding how they operate.

Highest Changes in Fraudulent Transaction Values by Key Subvertical

Fraudulent transaction values exploded in key subverticals between 2020-2021.

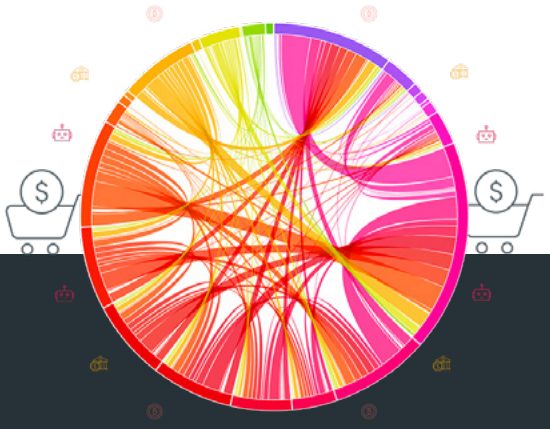
THE ANATOMY OF A FRAUD RING

Dissecting Abuse Tactics & Technologies

Fraud is a business, and cybercriminals are equally as invested in consumer behaviors, market trends, and emerging technologies as merchants. But because they view vulnerabilities as opportunities, fraudsters are less concerned with what's coming than they are with what's being ignored.

High-risk consumer behaviors, for example, are typically met with reactive tools, if they're noticed by merchants at all. Simple password creation requirements don't stop customers from reusing the same credentials across multiple websites, or opting to save passwords on websites where their payment info is also stored—which **38%** of consumers surveyed admit to doing.

These risks exist all along the customer journey, often going totally unchecked unless the business has applied friction and authentication throughout the site or app; but even these protections don't fully incapacitate fraud. Worse, they're not always accurate, and can lead to falsely-declined transactions and missed attacks that undermine other fraud prevention tactics merchants have put in place.



Sift's new Fraud Intelligence Center features fraud data from Sift's global network of 70 billion events per month. Discover expert tips, analyst resources, breaking industry news, and everything trust-and-safety to help fraud analysts and e-commerce leaders streamline security and ignite rapid growth.

Consumers react to online risk

The Fraud Economy sits just behind the veil of legitimate digital commerce. This global, interconnected network of online abuse causes rippling impact—in some cases, an attack against a single business can have repercussions for other merchants that aren't even in the same industry; a compromised set of credentials can help fraudsters subvert security across multiple sites. And, a profitable breach using one vector can turn out to be fundamental to the success of another—which is regularly the case when it comes to payment fraud.

Recently, Sift data scientists and fraud experts have surfaced, investigated, and taken down a number of fraud rings attempting attacks across our network, all employing multiple vectors and tools:

Pig Butchering. These operations are run by organizations of crypto-scammers who target dating sites, "plumping" up prey for their potential profitability through love-bombing and elaborate promises of crypto riches. Sift went undercover to stop them.

Proxy Phantom. This bot-savvy fraud ring deployed a series of global ATO attacks against multiple merchants simultaneously, applying automation to perform rapid credential stuffing and IP address rotation.

Cart Crasher. After setting up fake fundraisers on donation and giving sites (via born-bad accounts/ATO), this scam-driven fraud ring used bots to run stolen payment details through guest checkout, donating to their own illegitimate causes.

Below, we examine how these global attacks unfolded, and highlight shared characteristics across each.

Global Fraud Ring Tactics

Account takeover (ATO) | Payment abuse | Automation (bot attacks) | Content fraud

Pig Butchering

1. Create multiple fake dating profiles/crypto-investing platforms.
2. Target and woo victims on dating apps; push the conversation off-platform.
3. Convince victims to invest in fake crypto platforms; manipulate gains.
4. Scam victims out of thousands of dollars; abruptly cease communications.

Proxy Phantom

1. Buy/steal payment info and credentials.
2. Automate huge surges of login requests against multiple merchants.
3. Access accounts in seconds; mine for data/rewards points; make unauthorized purchases.
4. Compromise merchant security using automation and exposed data.

Cart Crasher

1. Use ATO/born-bad accounts; exploit guest checkout.
2. Create illegitmate fundraising posts using fake/stolen info.
3. Automate card testing using fake accounts/guest checkout; "donate" with stolen payment info.
4. Use verified stolen payment info elsewhere; solicit external donations to fake cause.

Mutual Attack Strategies

- Combined use of content fraud, ATO, and payment abuse.
- Attacks are rapid, distributed, and vector-agnostic.
- Exploit consumer risk (e.g., poor password hygiene, public chat forums).
- Use MFA- and CAPTCHA-dodging bots to test credentials and stolen payment info.
- Rely on automatic fulfillment and user-generated content to avoid security gates/plant scams.
- The goal is always financial gain.

In examining the techniques of these organized fraud rings, it's clear that the most sophisticated and damaging attacks leverage shared tactics and technologies. They don't stick to a single type of abuse, and they go after individual victims and businesses to gain ground for operations against entire communities of merchants and consumers. Fraudsters are also largely indiscriminate about what types of merchants they target, so long as there are profits to be made.

Trust and safety teams are the first and last line of defense against fraud. Adopting an end-to-end, real-time approach, backed by a network of billions of events, allows analysts to succeed and scale operations while propelling business growth with every transaction. Take our Digital Trust & Safety Assessment today.

About 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 DoorDash, Twitter, and CoinJar rely on Sift to catalyze growth and stop fraud before it starts. Visit us at sift.com, or follow us on LinkedIn.