sift

Q1 2023 DIGITAL
TRUST & SAFETY INDEX

Payment fraud data and insights from Sift's global network

Contents

NETWORK DATA 2021–2022

Payment fraud rises in fintech, digital goods & services

Payment fraud cost online businesses $41B USD globally in 2022. Those losses are expected to jump 17% in 2023, hitting $48B by the end of this year.

Of that massive debt, card-not-present (CNP) fraud is predicted to siphon $9.49B from digital merchants. That's a 57% increase in losses from 2019, and will make up 73% of all card-related losses in 2023. It's no longer a matter of *if* a business will face a payment fraud attack, but when, from where, at what scale, and for how long.

Despite **62%** lower order volumes YoY in fintech, financial services like buy now, pay later (BNPL), payment service providers (PSPs), and institutions like crypto exchanges are feeling the heat.

Sift network data shows that attempted payment fraud in fintech jumped **13%** between 2021 and 2022, with BNPL struggling against a **211%** increase, and crypto exchanges seeing a **45%** surge.

2022 VS. 2021

Increase in payment fraud rates: Key fintech subverticals

↑13%	↑211%	↑45%	↑35%	↑5%
All fintech	BNPL	Crypto exchanges	Loyalty	PSPs

It's no longer a matter of *if* a business will face a payment fraud attack, but when, from where, at what scale, and for how long.

Over 70% of all financial institutions reportedly lost at least $500k to payment fraud in 2022, with 91% of risk experts surveyed saying YoY fraud rates at their organizations are on the rise. Similarly, digital goods & services providers were hit by a **27%** uptick in payment fraud, with B2C merchants slammed by a **64%** spike.

Consumers are also under fire, with nearly half of them experiencing payment fraud within the past two years.

Worse, well over half of victims have been defrauded at least 2–4 times.

Rise in global payment fraud, 2022 vs. 2021

↑27% All digital goods & services

↑64% Business-to-consumer (B2C) digital goods & services

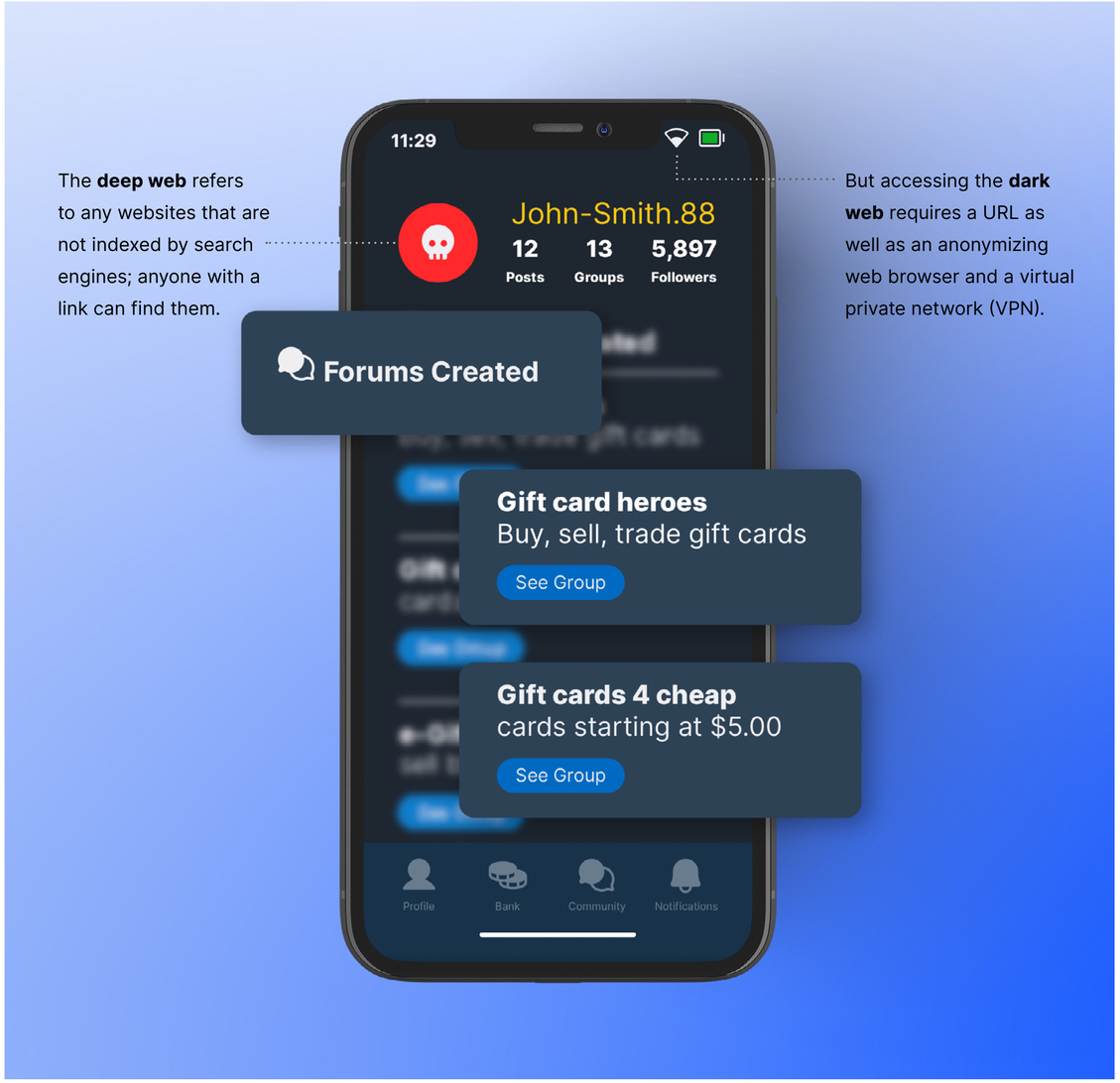
Consumers often become repeat victims

43% have recently fallen victim to payment fraud

62% have experienced payment fraud between 2–4 times

Recession fears feed marketplace fraud

Professional marketplaces have seen fluctuating transaction volumes in response to macroeconomic concerns. Buyers and businesses alike have shifted priorities, leading to widespread layoffs and tightened budgets. Fraudsters are taking advantage of the turmoil, driving the value of fraudulent transactions in professional marketplaces up **62%** YoY. Marketplaces in general saw average fraudulent transaction values jump **52%** YoY to **$5,149.82**. Those values also spiked **80%** on dating sites, **52%** on e-commerce marketplaces, and **18%** on social marketplaces.



CONSUMER INSIGHTS

The democratization of fraud meets FaaS (fraud-as-a-service)

FaaS (fraud-as-a-service) is the deep web's answer to the internet's evolving response to risk. Businesses are getting smarter and faster with trust and safety. This has led fraudsters to adopt e-commerce best practices, turning stolen data and proven attack methods into profitable—and marketable—products and services.

These schemes operate similarly to online marketplaces. Seasoned fraudsters sell on-demand services to other, sometimes first-time, culprits—a new wave of cybercriminals who have casually made it onto the deep and dark web.

In late 2022, researchers discovered a fraud ring, dubbed EvilProxy, that productized and monetized a phishing kit. Buyers could use it to "harvest valid session cookies and bypass the need to authenticate with usernames, passwords, and/or 2FA tokens," wiping out the necessity for specific skills and lowering the barrier to entry for less sophisticated fraudsters.

But FaaS isn't limited to phishing kits, and payment fraud doesn't start *or* stop with unauthorized purchases. Gift card fraud, promo abuse, card testing, card hopping, page- or code-jacking, first-party fraud and false returns, account takeover, and identity theft are only some of the types of abuse criminals leverage to commit payment attacks.

See one example of how this born-bad business model plays out on the next page.

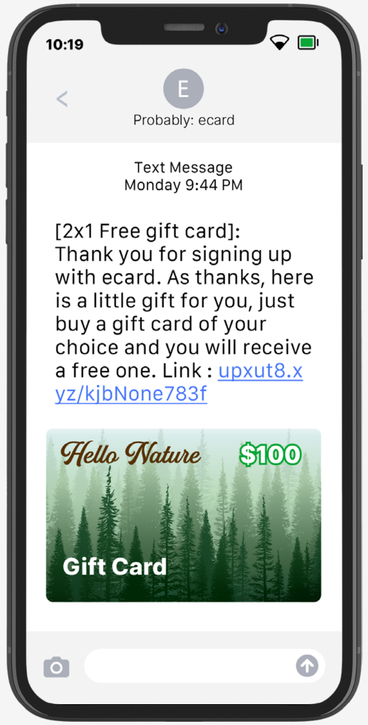
sift

FRAUD-AS-A-SERVICE

Mechanics of a criminal business model

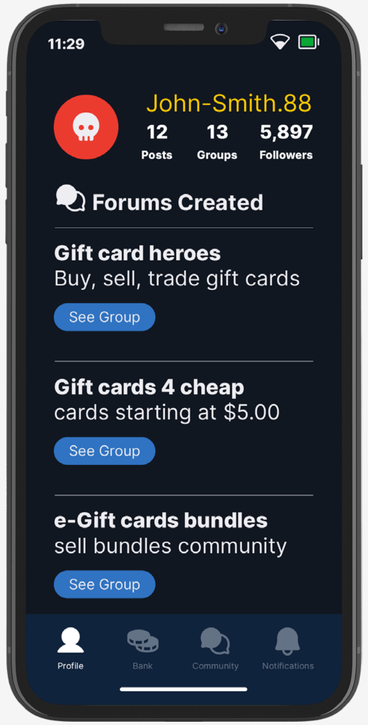
STEP 1

The fraudster steals e-gift card credentials via hacking, malware, or phishing.



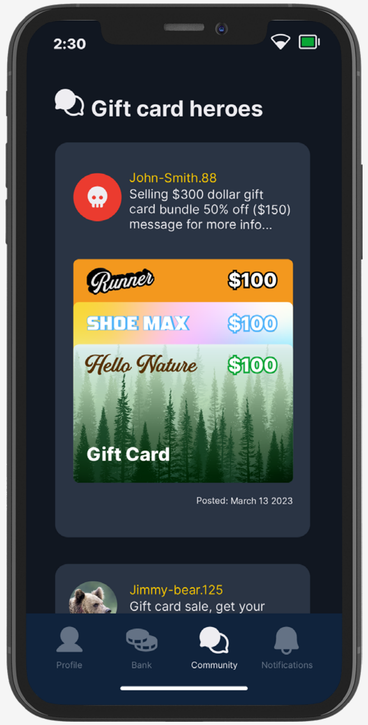
STEP 2

The fraudster creates or joins a group on a deep web forum and cultivates a following.



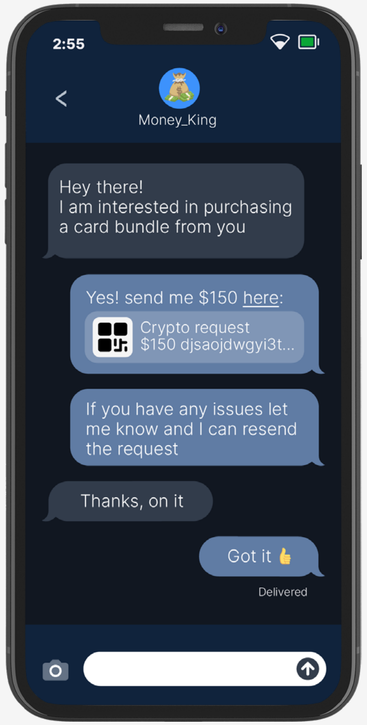
STEP 3

The fraudster advertises the e-gift cards to other fraudulent buyers at a deep discount.



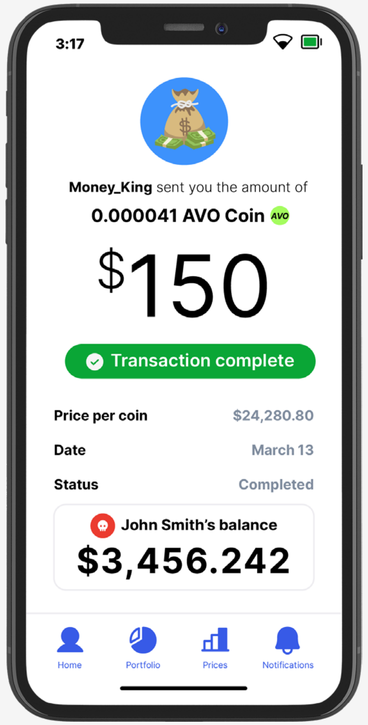
STEP 4

An opportunistic buyer agrees to purchase multiple e-gift cards at 50% off.



STEP 5

The buyer makes purchases with the stolen e-gift cards and the fraudster earns a profit.



Over **20%** of payment fraud victims don't know what happened to their payment data once it was compromised.

"FaaS attacks are a prime example of why merchants need the universal coverage offered by a diverse, real-time global network of fraud data covering multiple industries and regions," says Kevin Lee, VP of Trust & Safety at Sift. "Merchants face increasingly aggressive competition with each new player that enters the market. It's the same for the global Fraud Economy. Businesses can, and should, anticipate that fraud methodologies will evolve faster, and present a greater threat, as FaaS matures and becomes more competitive."

Fraudsters don't even need a dedicated pirating platform to collect exposed payment data. There's no shortage of it available for purchase: in 2022 alone, over 4,100 publicly disclosed data breaches took place globally, with approximately 22 billion customer records compromised in the process.

Whoever's willing to buy that kind of data can do so. That includes consumers who seize the occasional opportunity to steal online—which **16%** admit to having done (or having known someone who has). Another **17%** have encountered online offers to commit fraud, whether they accepted or not.

The fact that nearly **one-fifth of consumers admit to committing or know someone who has committed payment fraud** is a glaring sign of the rapid democratization of fraud. Just like software providers that work to make their platforms accessible to more users throughout a business, fraudsters have demystified the tools and tactics they use to steal, making them both easy to find and easy to use for anyone with internet access.

This democratization has done more than make it simpler to hijack digital data. It's also opened up new revenue streams for seasoned cybercriminals that go beyond pointed attacks. Along with an increase in bad actors attempting to "recruit" consumers on platforms like Telegram and TikTok, fraudsters can now scale their own efforts while profiting from the expansion—in addition to reaping the rewards of successful breaches.

When attacks do succeed, the damage to both merchants and consumers is immediate and long-lasting.

Twenty percent of payment fraud victims don't know what happened to their information after it was exposed. They're entirely unaware of who has their personal data or how much of it they've accessed, what the fraudster has been able to find out about them or their online activity, or how the data is being leveraged against businesses and other consumers.

Consumer confessions and deep web recruiting

16% of consumers admit to having committed payment fraud/knowing someone who has

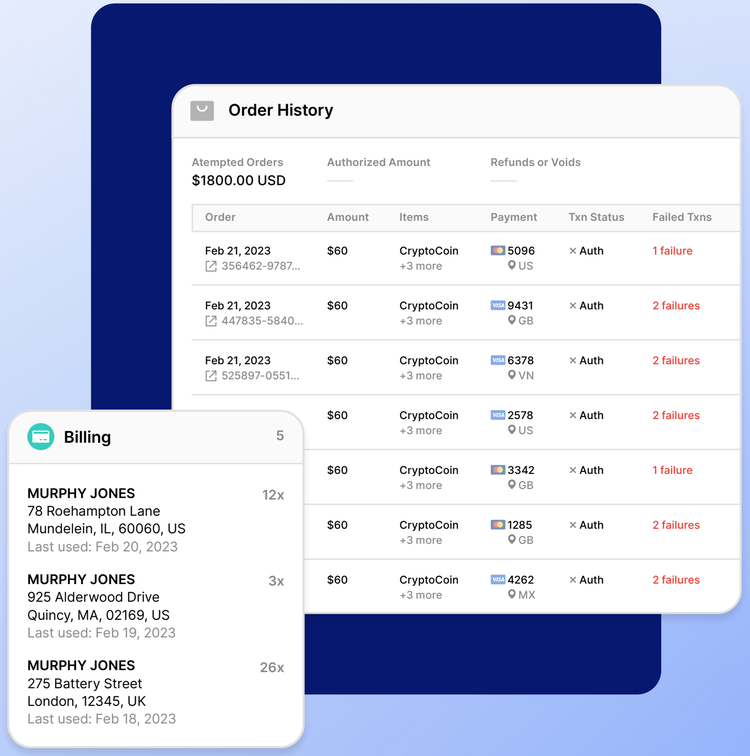
17% of consumers have seen offers online to participate in payment fraud

This compromised payment information can be used immediately to buy/liquidate goods or cryptocurrency. It can be collected for use at a later time, or to complete fake credentials. It can also end up on the deep or dark web, sold in bulk alongside similar data—a valuable asset for committing attacks at speed and scale.

Sift experts recently red-flagged evidence across the network of cybercriminals attempting to leverage a classic financial tactic known as **card hopping**. Typically, this refers to consumers opening multiple new credit lines or bank accounts to take advantage of offers that immediately benefit the new cardholder.

But when fraudsters card hop, it's with the intent to obtain a tangible payout in money or merchandise using compromised payment data. Unlike the more direct attack method of card testing, which helps validate that hacked payment methods are active via rapid-fire, low-value, automated transactions, **card hopping** involves using those confirmed cards to make full-value unauthorized purchases or withdrawals.

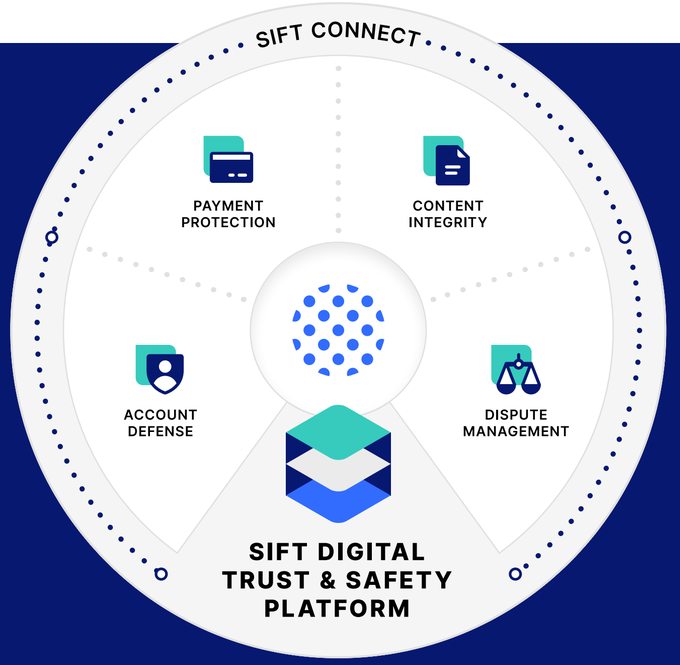
Data scientists pinpoint risky signals and schemes using Sift's global network



> Most consumers—**64%**—report using only a couple of payment cards every month, with fewer than **5%** using at least five cards per month. But fraudsters can use up to two-to-three times the cards during the same timeframe, and each of those payment methods is usually tied to a higher-than-average number of failed transactions. That's exactly what alerted us to the risk. And because the activity can appear natural, it can be much easier for fraud teams to miss.

Jane Lee, Sift Trust and Safety Architect

Companies that adopt an end-to-end, real-time approach, backed by a network of global signals and events, reduce block rates by **55%*** compared to those that don't.



Fraudsters can more easily avoid detection this way, because while the actions can still be automated, their behavior will appear closer to natural than a large-scale/small value card testing attack. And because the activity may not immediately signal risk, merchants struggle to accurately detect it.

Sift data scientists also noted that card hoppers typically kept **at least five payment cards** in rotation each month from disparate providers and regions, even when associated with repeat IP and mailing addresses. Consumers validated that this behavior was suspicious, reporting that they only use **1–2 payment cards** during a normal month.

Sift Trust & Safety Architects also point out that while individual fraudsters can, and do, execute card hopping schemes, it's the collaboration between bad actors in the Fraud Economy that compounds the risk and its reach. "We uncovered that individual users with more than five cards in rotation every month also had multiple addresses associated with their payments—many issued from financial institutions in different regions," said Jane Lee. "It's unusual for one consumer to have payment methods from several regions or countries. This suggests that fraudsters are working together to target individuals and institutions from all over the world to obtain and exploit exposed data regardless of location."

Increased accessibility to FaaS, forums, and lists of hacked data present more opportunities for motivated criminals—and criminal-consumers—to exploit leaked information. That makes trust and safety operations the single point of failure or success for a business, and ongoing economic uncertainty means that merchants are having to do more with less.

Analysts need the right tools to successfully stop payment fraud and scale operations, all while fueling faster growth with every transaction. **Take control of payment fraud with Sift's Digital Trust & Safety Platform. Schedule time with us today.**

**The data highlighted in this report is derived from Sift's global data network of one trillion (1T) events across 2021 and 2022, along with insights gathered on behalf of Sift by Researchscape, which polled 1,091 (aged 18+) U.S. consumers (aged 18+) in February 2023.*

Sift is the leader in Digital Trust & Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of one trillion (1T) events per year, and a commitment to long-term customer partnerships. Global brands such as DoorDash, Twitter, and Wayfair rely on Sift to gain a competitive advantage in their markets. Visit us at **sift.com**, and follow us on **LinkedIn**.

© 2022–2023 Sift Science, Inc. All rights reserved. Sift and the Sift logo are trademarks or registered trademarks of Sift Science, Inc.