sift

Q3 2023 DIGITAL TRUST & SAFETY INDEX

Account takeover data, consumer insights, and emerging trends

Login Failed

Too many login attempts. Account locked.

OK

Contents

02
2023 industry and consumer insights

06
Findings, fraud rings, and future predictons

ACCOUNT TAKEOVER

2023 INDUSTRY AND CONSUMER INSIGHTS

Account takeovers strike fintech, food & beverage

Predictions point to billions in fraud losses by the end of 2023, with over $635B related to account takeover (ATO) attacks. The data tracks: ATO attacks jumped an eye-popping **354%** year-over-year in Q2 2023 across Sift's global network, after an already concerning **169%** increase YoY in 2022.

Evolving tools like generative AI mean businesses in every region and vertical are facing faster, costlier attacks, and losing ground when it comes to accurately detecting abuse. Fraudsters can use it to snatch data in seconds and disappear into anonymity just as quickly, making automation central to some of the most widespread and costly account takeover attacks launched against digital businesses.

↑354%

increase in ATO attacks year-over-year in Q2 2023 across Sift's global network.

Source: Sift global data network. ©2023

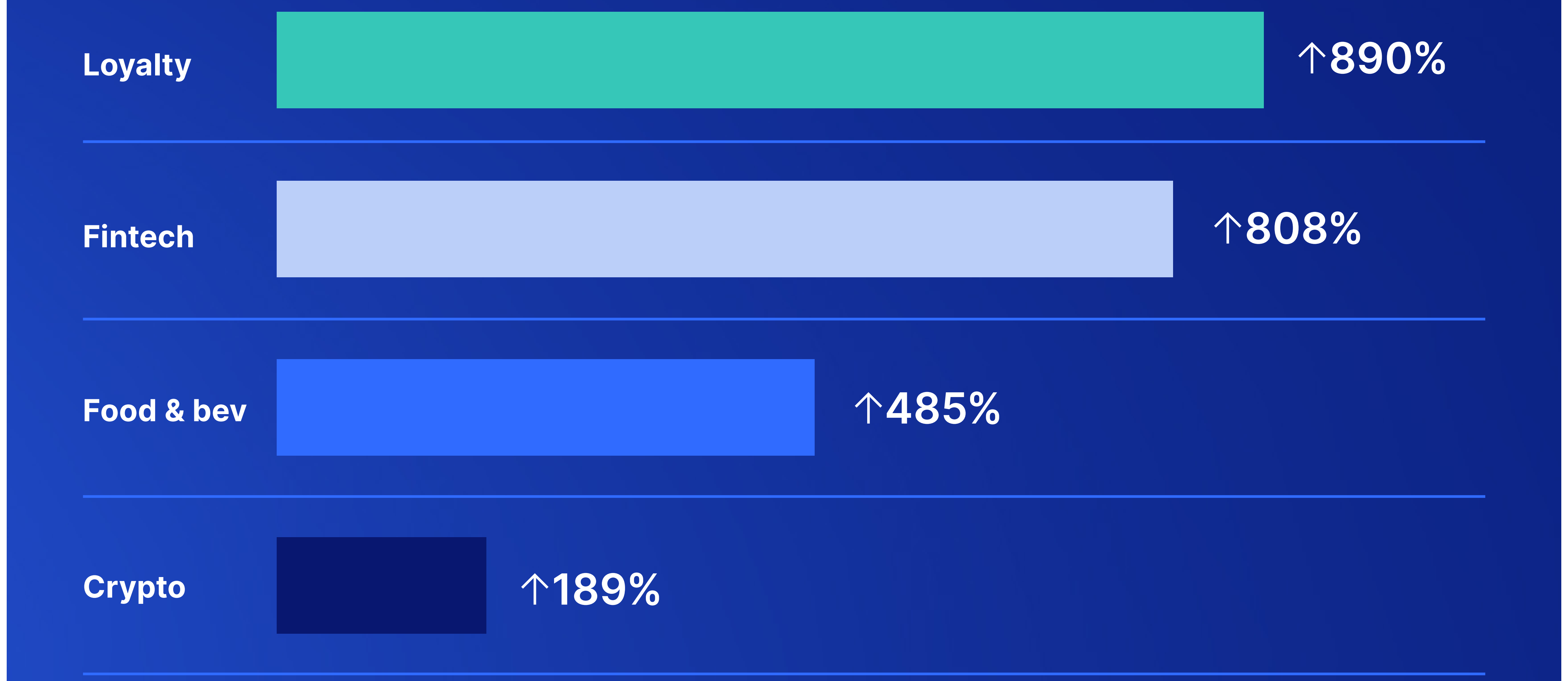
At the same time, the global Fraud Economy has produced the tactics and tools necessary to target industries where growth is rapid and consumer investment in security is high—like fintech, where ATO spiked **808%** YoY*, pummeling loyalty and crypto and opening the gate to downstream payment fraud.

Fintech's volatility is well-known, thanks to constant coverage of Bitcoin-based scams and crypto winters. An uptick in crypto-related account takeover—especially under a huge swell across the industry as a whole—comes with the territory. But fraudsters' focus on loyalty merchants (sites/apps that reward users for online and offline shopping) was unmatched, launching account takeover rates nearly **900% higher** than they were this time last year.

**All proprietary 2023 Sift network data in this report compares information from Q2 2022 to information from Q2 2023 unless otherwise stated.*

Post-pandemic, permanent adoption of digital ordering and delivery services continues to create opportunities for cybercriminals to exploit customer information. Account takeover attack rates jumped almost **500%** YoY for food and beverage brands, on the tail of COVID-fueled growth for kingpin QSRs (quick-service restaurants) and small businesses alike. For some, that demand scaled faster than security awareness or digital transformation, leaving merchants at the mercy of ATO fraudsters.

Increase in ATO by vertical across Sift's global network, Q2 2022 compared to Q2 2023



Source: Sift global data network. ©2023

The recent meteoric rise in ATO likely influenced rising payment fraud in early 2023, and consumers felt the heat.

Nearly one-fifth (18%) of those surveyed by Sift have experienced account takeover attacks, with **62%** of those taking place in the past year. Over **34%** of victims were defrauded **2+ times**, typically while using sites or apps for **digital subscriptions**, **online shopping**, and **financial services**.

Payment fraud was the universal outcome of these attacks: **over two-thirds** of victims reported unauthorized purchases made with exposed payment details, while **one-fourth** of those impacted had stored funds drained from the affected account.

Top 3 sites at risk for account takeover

According to consumers. Respondents could select multiple options.

Source: Sift global data network. ©2023

36%
Subscriptions for digital services

31%
Online shopping

29%
Bank or credit account

Consumer credentials are easy to crack

Poor password hygiene is a leading catalyst for account-based fraud, and consumers readily admit to it. Google found that 65% of Americans reuse passwords, 20% use common or easily guessable ones, and 52% include discoverable personal information; about 1 in 3 have shared or accessed someone else's password.

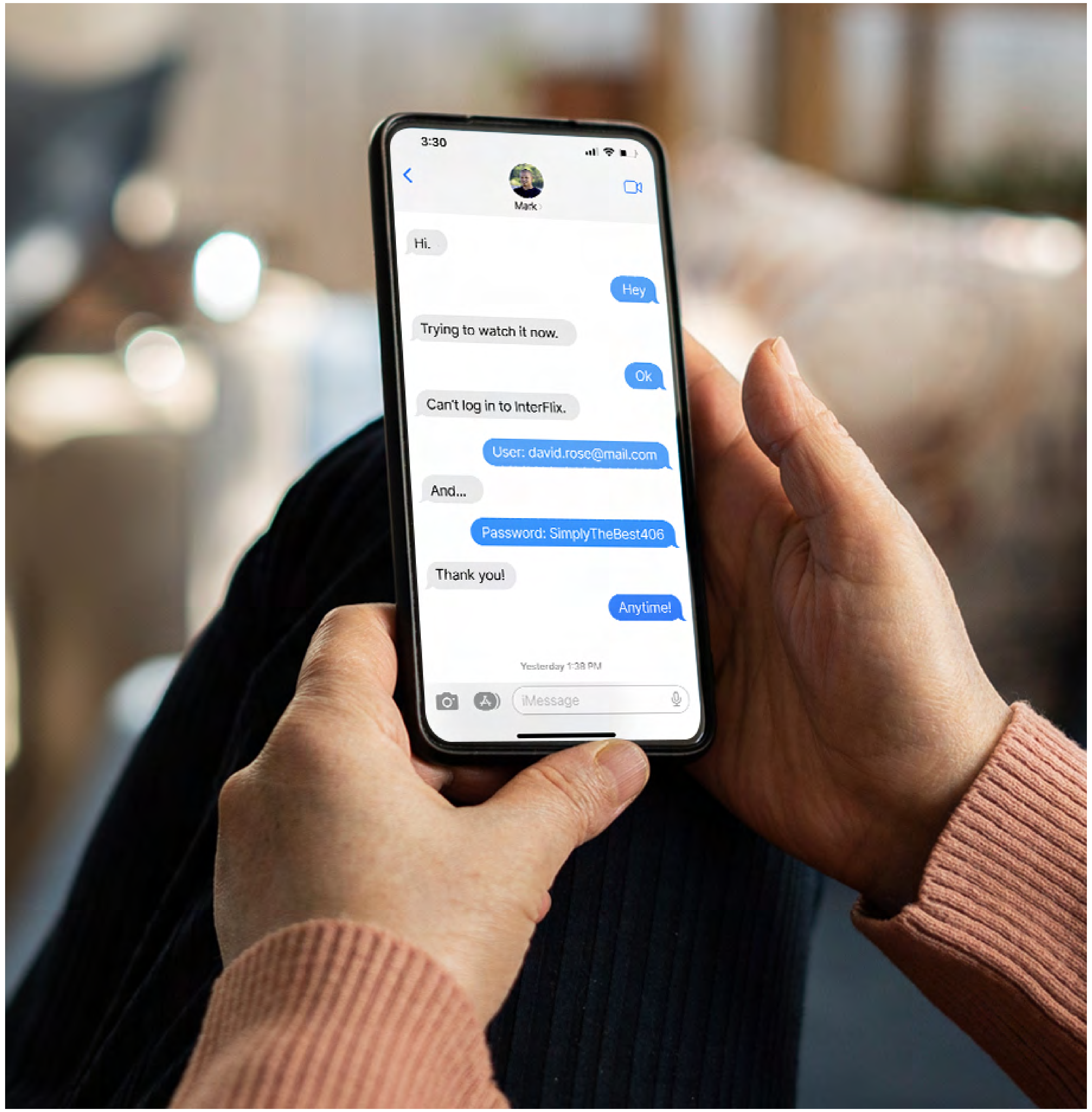
A Sift survey uncovered where the majority of credential reuse is taking place: **43%** of consumers recycle login info across online shopping sites, **38%** do so for digital subscriptions, and **28%** on utilities sites and apps.

Account takeovers can lead to multiple types of downstream payment fraud

67% of ATO victims' exposed data was used for unauthorized purchases

24% of victims had stored funds drained from the compromised account

Source: Sift global data network. ©2023



Hi.

Hey

Trying to watch it now.

Ok

Can't log in to InterFlix.

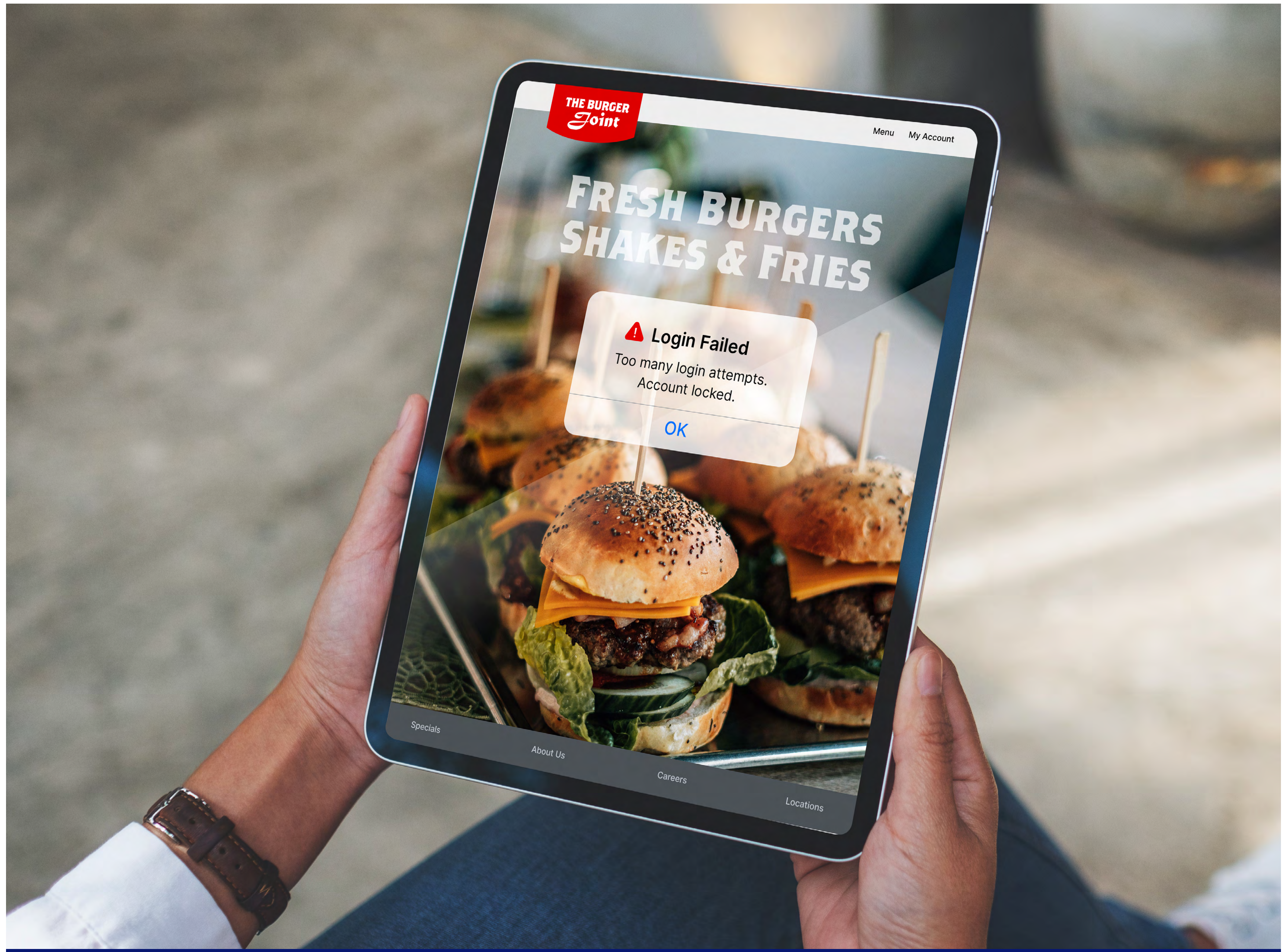
User: david.rose@mail.com

And...

Password: SimplyTheBest406

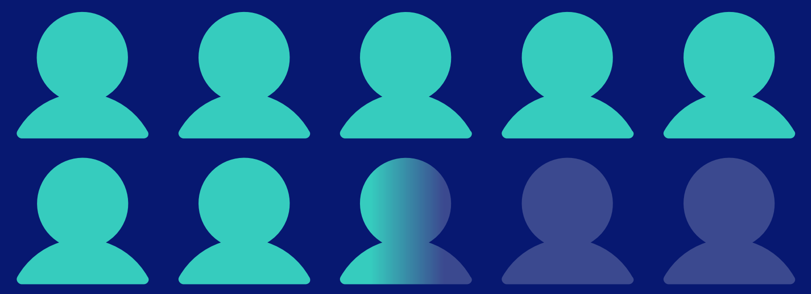
Thank you!

Anytime!



Login Failed

Too many login attempts. Account locked.



76%

of consumers would abandon a brand due to account takeover

Source: Sift global data network. ©2023

Most consumers (**73%**) believe the brand is accountable for ATO attacks and responsible for protecting account credentials; fewer than half (**43%**) of account takeover victims were notified by the company that their information had been compromised.

Exposing data—and selling it on the dark web—isn't where these attacks end. That data can be used on the breached site, across the internet, and in brick-and-mortar businesses. The longer consumer victims of ATO remain unaware, the more time fraudsters have to exploit the information they've uncovered to conduct unauthorized purchases and other transactions.

Failing to alert users that their credentials have been exposed is a risky choice for the impacted business in the short-term, inviting chargebacks and inventory theft, and can open the business up to fines and legal action.

Worse, it's a missed opportunity to prevent future churn and revenue loss: **over three-fourths of consumers would permanently stop shopping with a brand** if they became a victim of ATO via that company's site or app.

FINDINGS & PREDICTIONS

AI, automation, and ATO-as-a-Service

Artificial intelligence and automation are closely tied, but they're not the same. While both improve efficiency and reduce human involvement in tasks, AI extends the power of automation by introducing true learning capabilities and independent decision-making. Automation is rules-based, while AI is adaptable and can handle more complex asks—making it ideal for broader applications.

Generative AI is creating a universe of new possibilities for fraudsters, taking over where automation started to plateau. Standard-issue bots significantly reduce time and effort spent on execution tasks, like swapping IP addresses during an attack or rapidly testing credit card numbers. But emerging AI can produce conversational, grammatically correct text, images, and audio in minutes that are often indistinguishable from human writing and speech. It gives bad actors good coverage to launch campaigns designed to covertly gather account credentials.

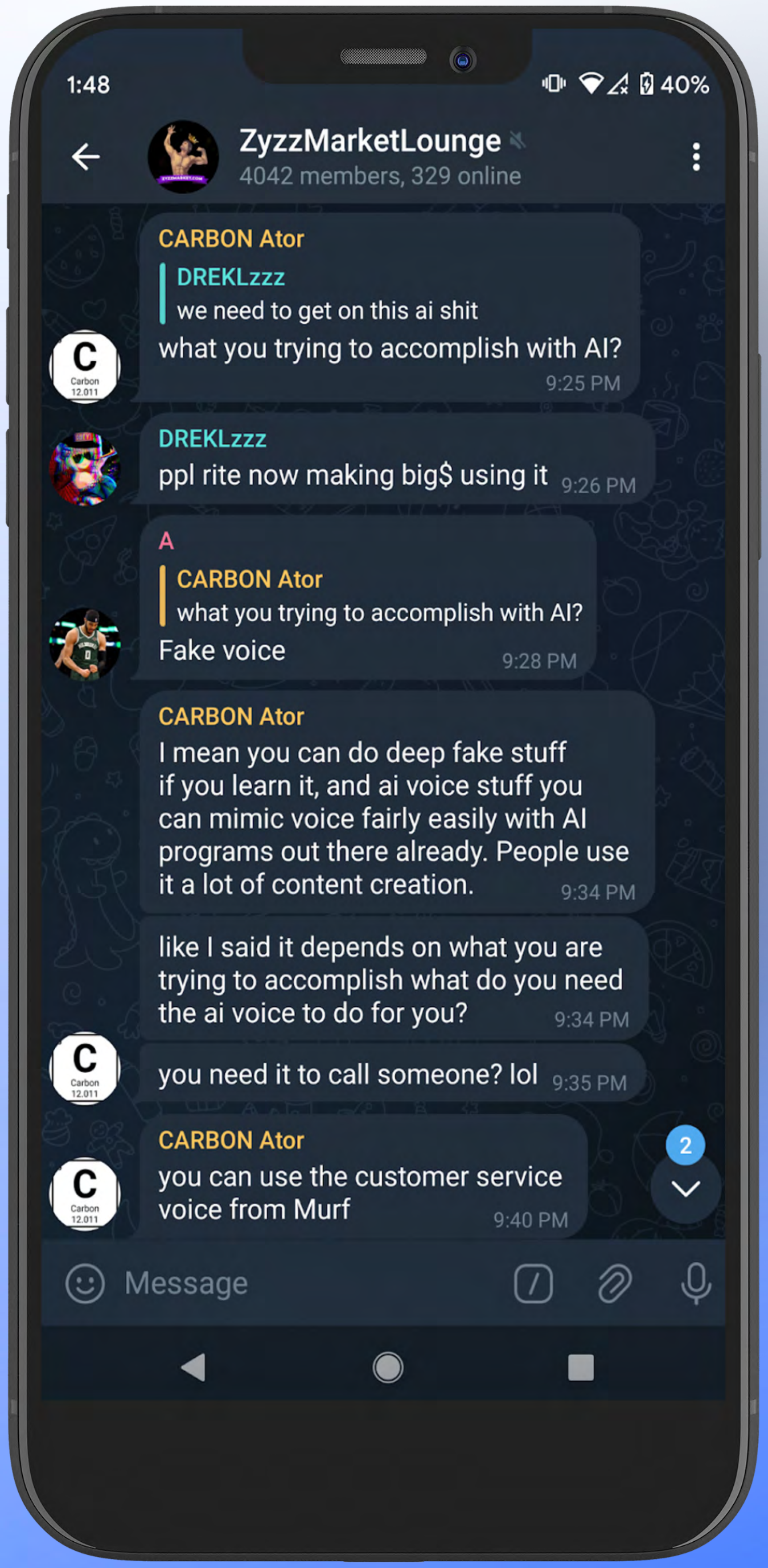
Still, while AI tools are making scams more sophisticated and convincing, many fraudsters are aggressive, efficient, and successful without them.

Regardless of how many phishing messages AI can produce, or how quickly, it hasn't reached a level of ease or scalability necessary to facilitate deep fakes or complex attacks without significant human oversight.

Found online: Criminal conversations in action

Sift Trust and Safety Architects regularly uncover conversations between bad actors claiming that configuring AI to execute campaigns takes too much time and effort to be a primary attack tool.

Scale is often the most important component of any scam for bad actors, who prioritize the size of the potential payout above how long it takes to get it. And like any digital business, they turn to social media to boost profits through marketing and recruiting—advertising schemes for fellow fraudsters to join, pushing fraud-as-a-service, and giving anyone who wants it access to illicit tools and tactics.



CARBON Ator
DREKLzzz
we need to get on this ai shit
what you trying to accomplish with AI? 9:25 PM

DREKLzzz
ppl rite now making big$ using it 9:26 PM

A
CARBON Ator
what you trying to accomplish with AI?
Fake voice 9:28 PM

CARBON Ator
I mean you can do deep fake stuff if you learn it, and ai voice stuff you can mimic voice fairly easily with AI programs out there already. People use it a lot of content creation. 9:34 PM

like I said it depends on what you are trying to accomplish what do you need the ai voice to do for you? 9:34 PM

you need it to call someone? lol 9:35 PM

CARBON Ator
you can use the customer service voice from Murf 9:40 PM

Source: Mobile screenshots used in this report were provided by Sift Trust and Safety Architects, uncovered during investigative research. ©2023

Of consumers surveyed by Sift, **24%** report having seen offers to participate in account takeover schemes online. These offers are often similar to job posts in career boards and chat groups. In this example uncovered by Sift Trust and Safety Architects, these cybercrime classifieds drive people directly to sites like Telegram, where they can easily join profitable fraud schemes.

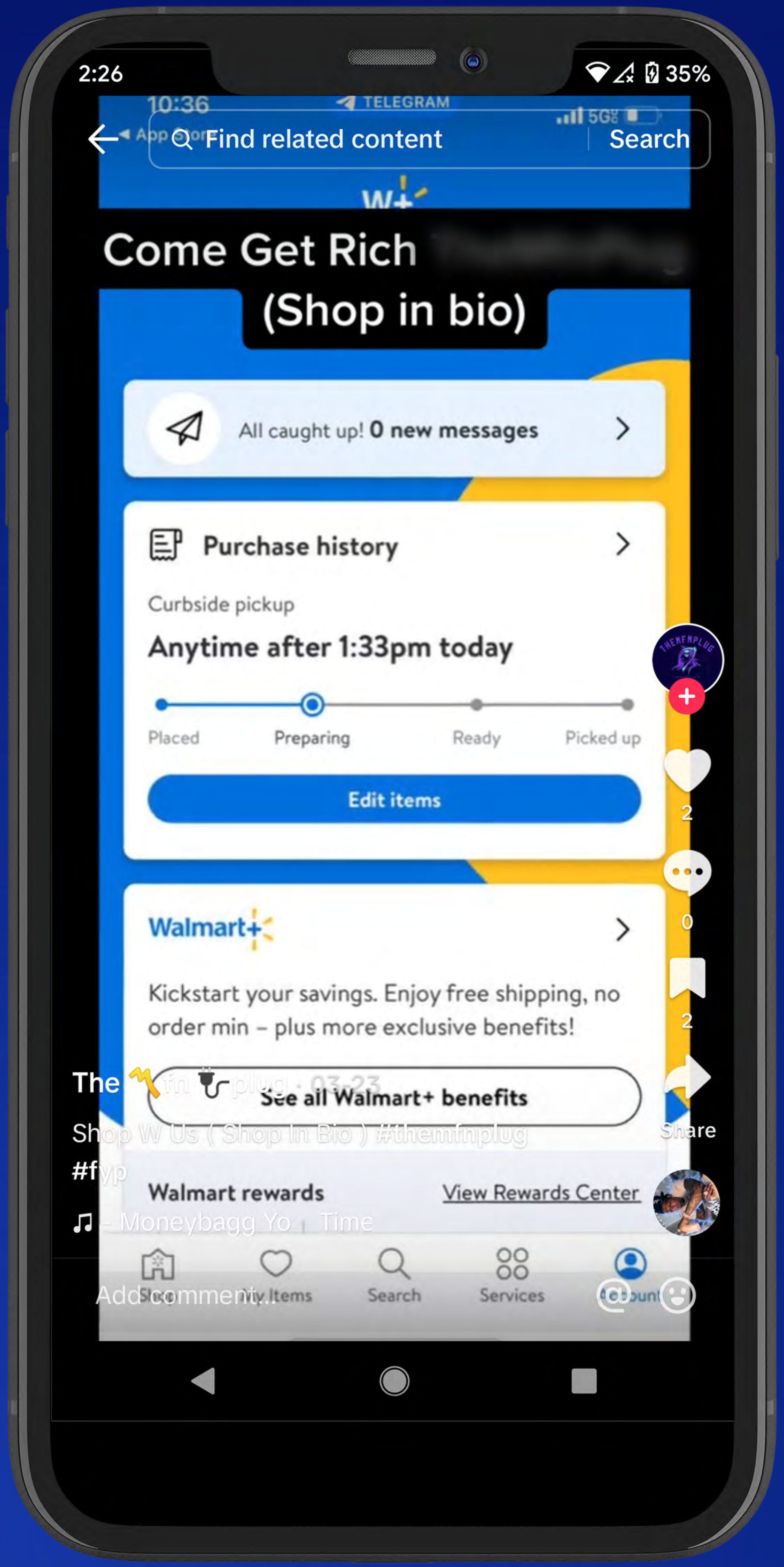
Unlike messages crafted to hijack consumer data, these "ads" are designed to attract players to participate in scams and other forms of online abuse. But because the advertisers cast a wide net across both the dark and open web—using social media as a marketing channel to drive people off-platform—professional fraudsters aren't the only ones who respond.

Sift experts refer to this phenomenon of openly advertised calls-to-abuse as the democratization of fraud—a growing accessibility and simplicity that allows anyone with internet access to participate in fraud. And some take the bait: **14%** of consumers say they know someone who has intentionally committed account takeover fraud, and **4%** admit to having purposely committed ATO themselves.

Referrals from TikTok to Telegram

Fraudsters find each other on popular messaging apps, covertly collaborating on promo abuse, payment fraud, and account takeover-based campaigns that siphon revenue from digital businesses.

For the most successful schemers, it's not about followers, but engagement and reach—and getting users off-platform to a messaging service, where the real collaboration can take place. Sift experts discovered that this is a specialty for one well-known criminal currently haunting the internet, whose Telegram channel boasts over 20k subscribers.



Come Get Rich [redacted]

(Shop in bio)

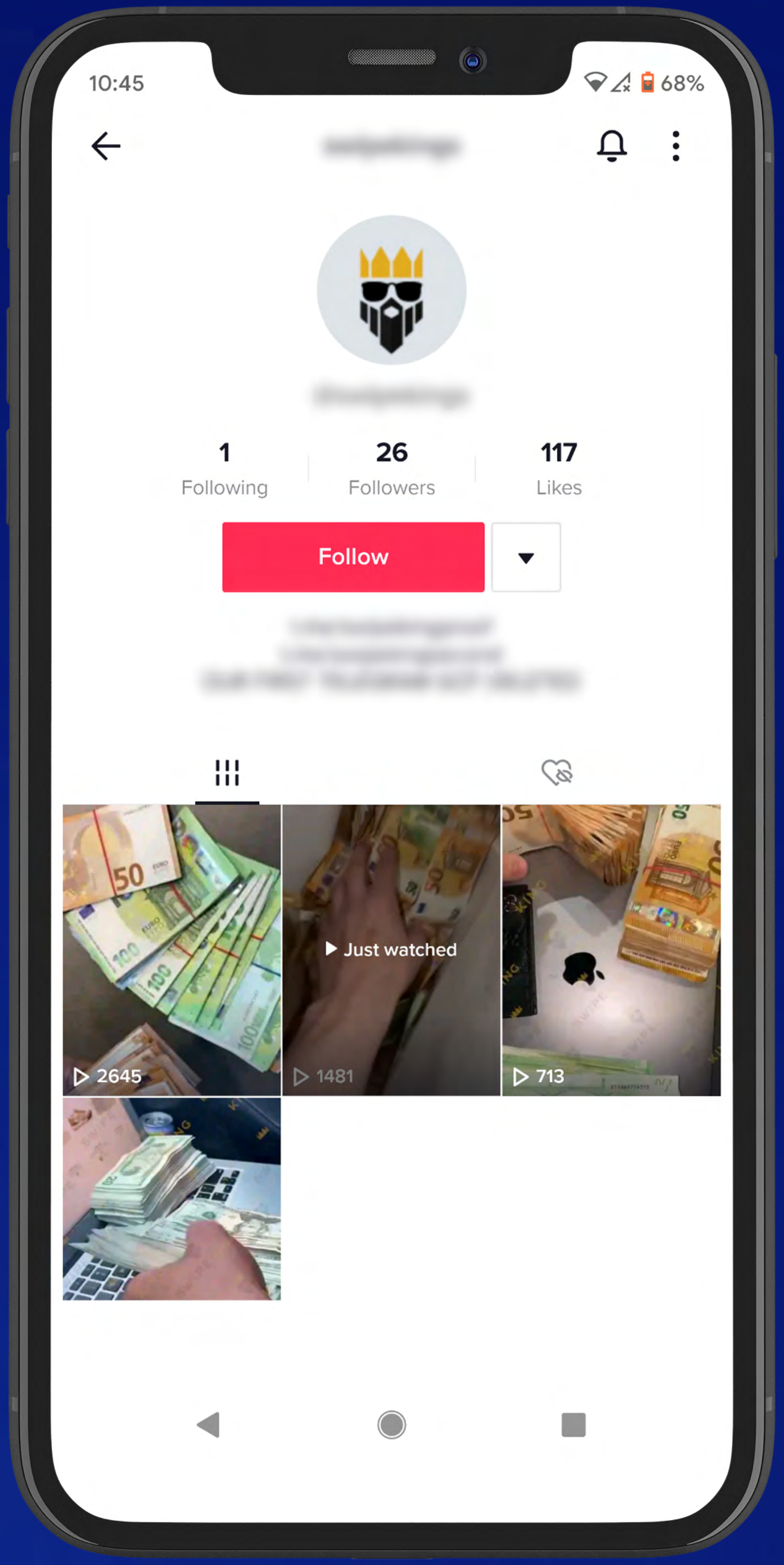
All caught up! 0 new messages

Purchase history

Curbside pickup

Anytime after 1:33pm today

Kickstart your savings. Enjoy free shipping, no order min – plus more exclusive benefits!



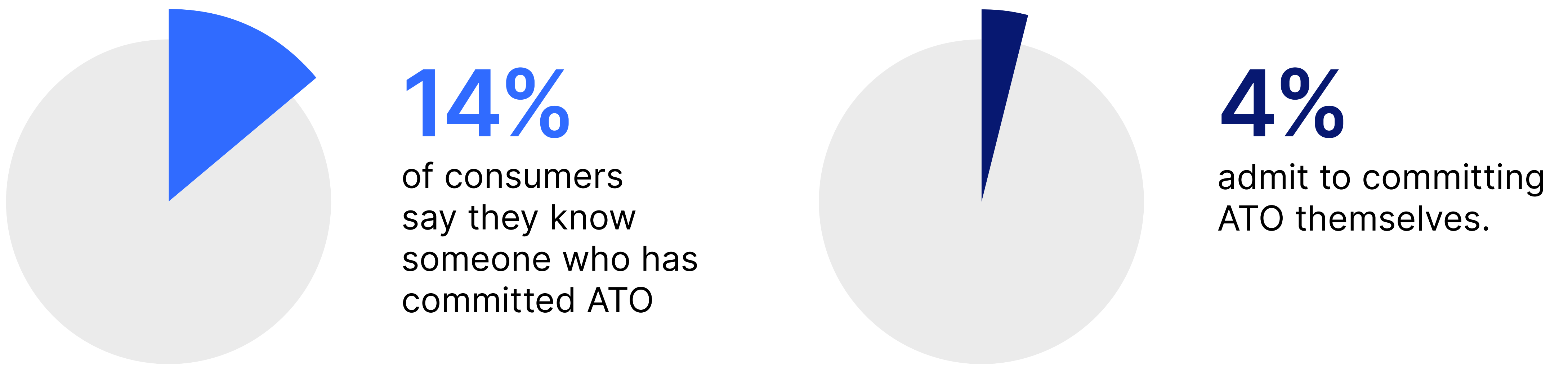
Source: Mobile screenshots used in this report were provided by Sift Trust and Safety Architects, uncovered during investigative research. ©2023

> Fraud becomes as sophisticated as the technology being used to commit it, and increasingly innovative types of automation pose a threat to merchants that aren’t ready to match its speed or account for its accessibility.
>
> But even discounting concerns over artificial intelligence-powered fraud, digital risk is growing in lockstep with e-commerce expansion. Highly organized, well-funded attackers present a worst-case scenario for businesses. Existing tools and tactics are doing long-term damage to users and merchants already, with perpetual potential to improve. Machine learning and data consortiums should be the foundation for businesses looking to both manage digital risk and drive growth.

Rebecca Alter
Sift Trust and Safety Architect

Coupling cutting-edge automation with democratized access has resulted in new fraud-as-a-service offers being added to an already-bloated Fraud Economy.

Consumers admit to ATO



14%
of consumers say they know someone who has committed ATO

4%
admit to committing ATO themselves.

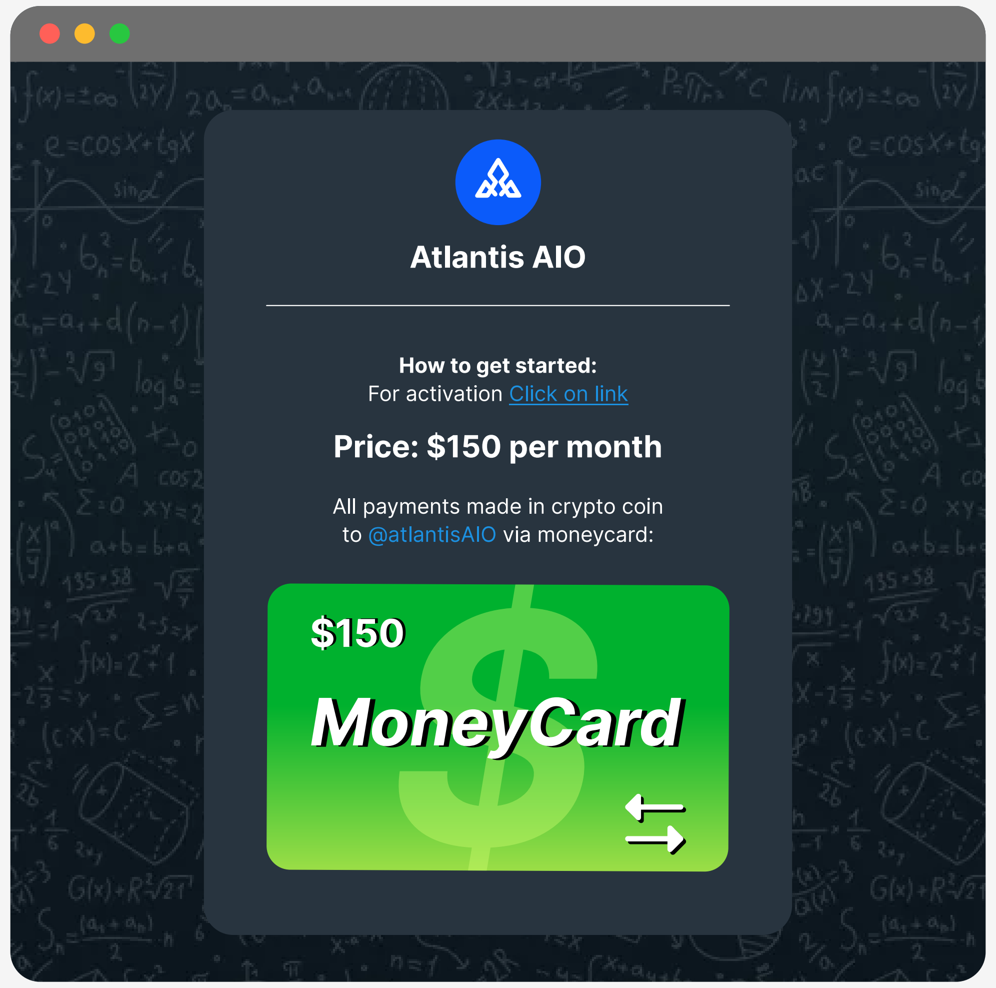
Source: Sift global data network. ©2023

Recently, Sift Trust and Safety Architects uncovered a tool on Telegram known as “Atlantis AIO.” Accessible through a link and priced at $150 per month, it’s a comprehensive credential stuffing service, used to check data against a wide range of companies and services.

Automation accelerates ATO-as-a-Service

Atlantis AIO (also known as Atlantis-X) is a fraud-as-a-service credential stuffing tool, accessible via a simple link for $150 per month. It allows fraudsters to test the validity of compromised credentials they've acquired against various businesses, both rapidly and at scale. What sets Atlantis AIO apart is its extensive list of supported sites, along with regular updates that help prevent the tool from being blocked by targeted companies.

STEP 1



Atlantis AIO

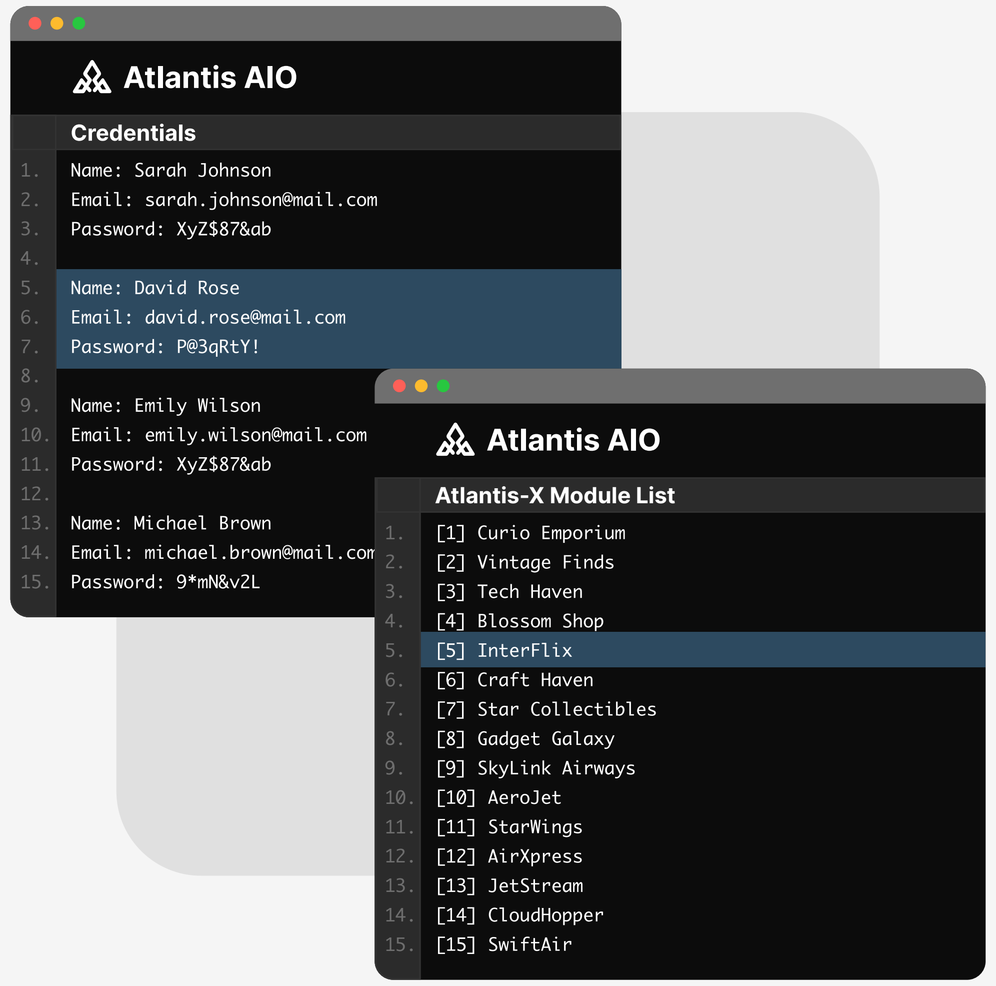
How to get started:
For activation Click on link

Price: $150 per month

All payments made in crypto coin
to @atlantisAIO via moneycard:

After being given the Atlantis AIO link through direct message, a fraudster pays the $150 monthly subscription fee. It's common for users to sign up using cryptocurrency, adding a layer of anonymity to the transaction.

STEP 2



Atlantis AIO

Credentials

```
Name: Sarah Johnson
Email: sarah.johnson@mail.com
Password: XyZ$87&ab

Name: David Rose
Email: david.rose@mail.com
Password: P@3qRtY!

Name: Emily Wilson
Email: emily.wilson@mail.com
Password: XyZ$87&ab

Name: Michael Brown
Email: michael.brown@mail.com
Password: 9*mN&v2L
```

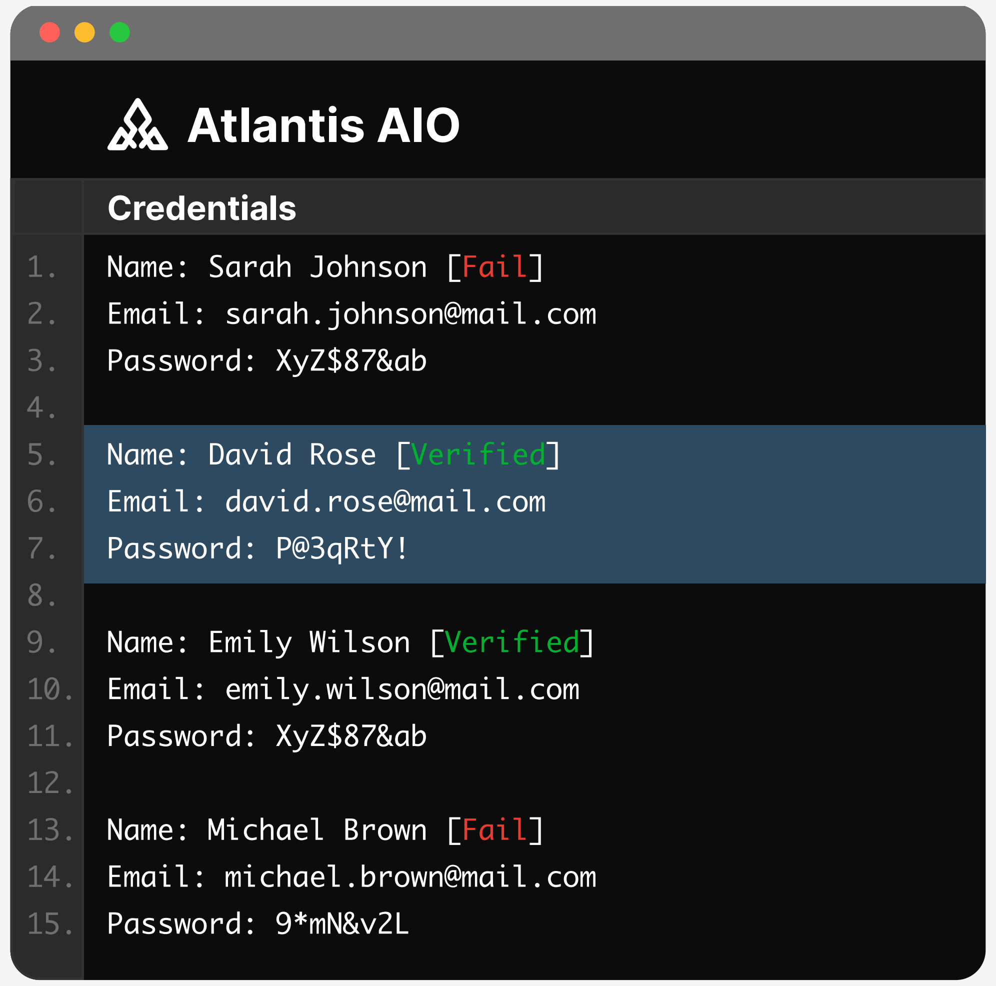
Atlantis AIO

Atlantis-X Module List

```
[1] Curio Emporium
[2] Vintage Finds
[3] Tech Haven
[4] Blossom Shop
[5] InterFlix
[6] Craft Haven
[7] Star Collectibles
[8] Gadget Galaxy
[9] SkyLink Airways
[10] AeroJet
[11] StarWings
[12] AirXpress
[13] JetStream
[14] CloudHopper
[15] SwiftAir
```

Behind the paywall, the fraudster enters the stolen or purchased account credentials, in bulk, into the Atlantis tool. Then, the fraudster selects which of the available sites they want to check the information against.

STEP 3



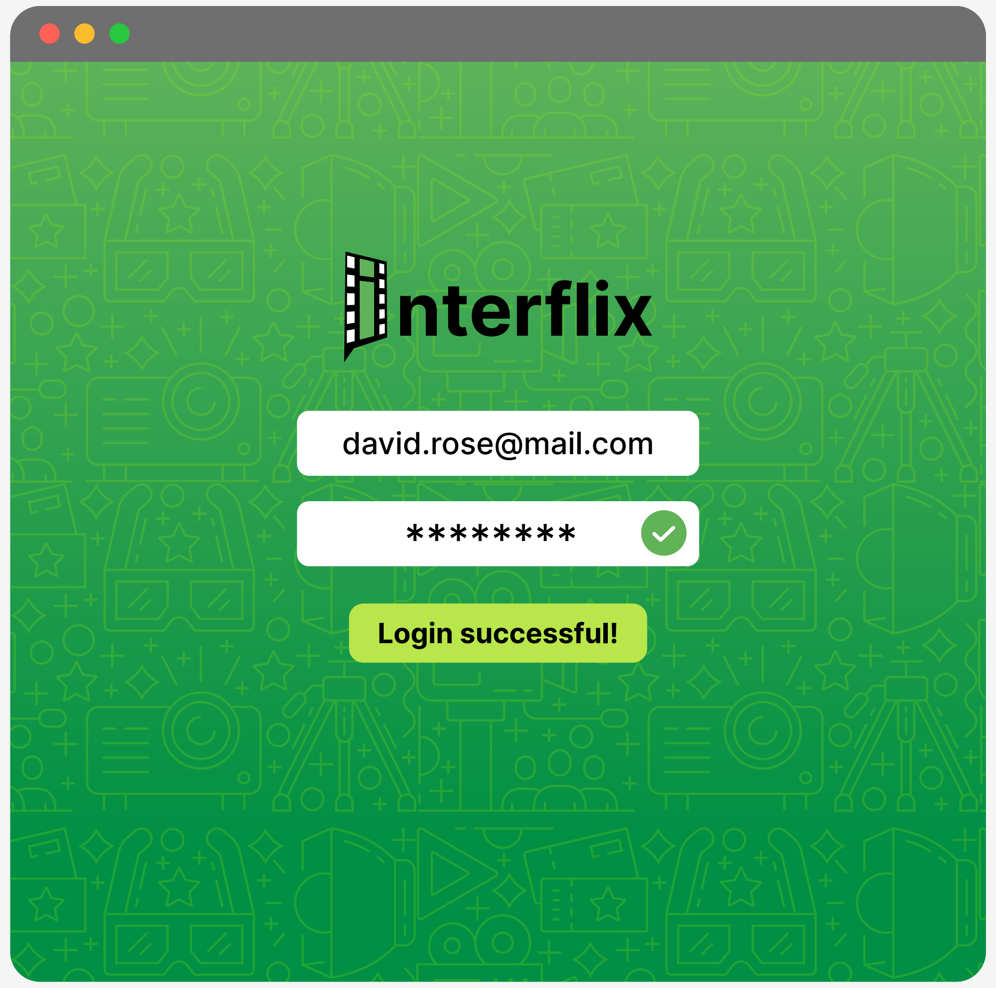
Atlantis AIO

Credentials

```
Name: Sarah Johnson [Fail]
Email: sarah.johnson@mail.com
Password: XyZ$87&ab

Name: David Rose [Verified]
Email: david.rose@mail.com
Password: P@3qRtY!

Name: Emily Wilson [Verified]
Email: emily.wilson@mail.com
Password: XyZ$87&ab

Name: Michael Brown [Fail]
Email: michael.brown@mail.com
Password: 9*mN&v2L
```

Atlantis applies automation to rapidly verify if, and where, those credentials are accurate and active. The tool does more than confirm whether the credentials work—it can also return account and loyalty point balances.

STEP 4



Interflix

david.rose@mail.com

******** ✓

Login successful!

The fraudster takes the Atlantis-authenticated data to the related websites or apps, quickly and easily accessing the compromised accounts, as well as any points, discounts, funds, or other details stored behind the gate.

Source: Mobile screenshots used in this report were provided by Sift Trust and Safety Architects, uncovered during investigative research. ©2023

Global fraud losses are projected to be 20% higher than they were last year, and set to cost merchants and consumers billions by the close of 2023.

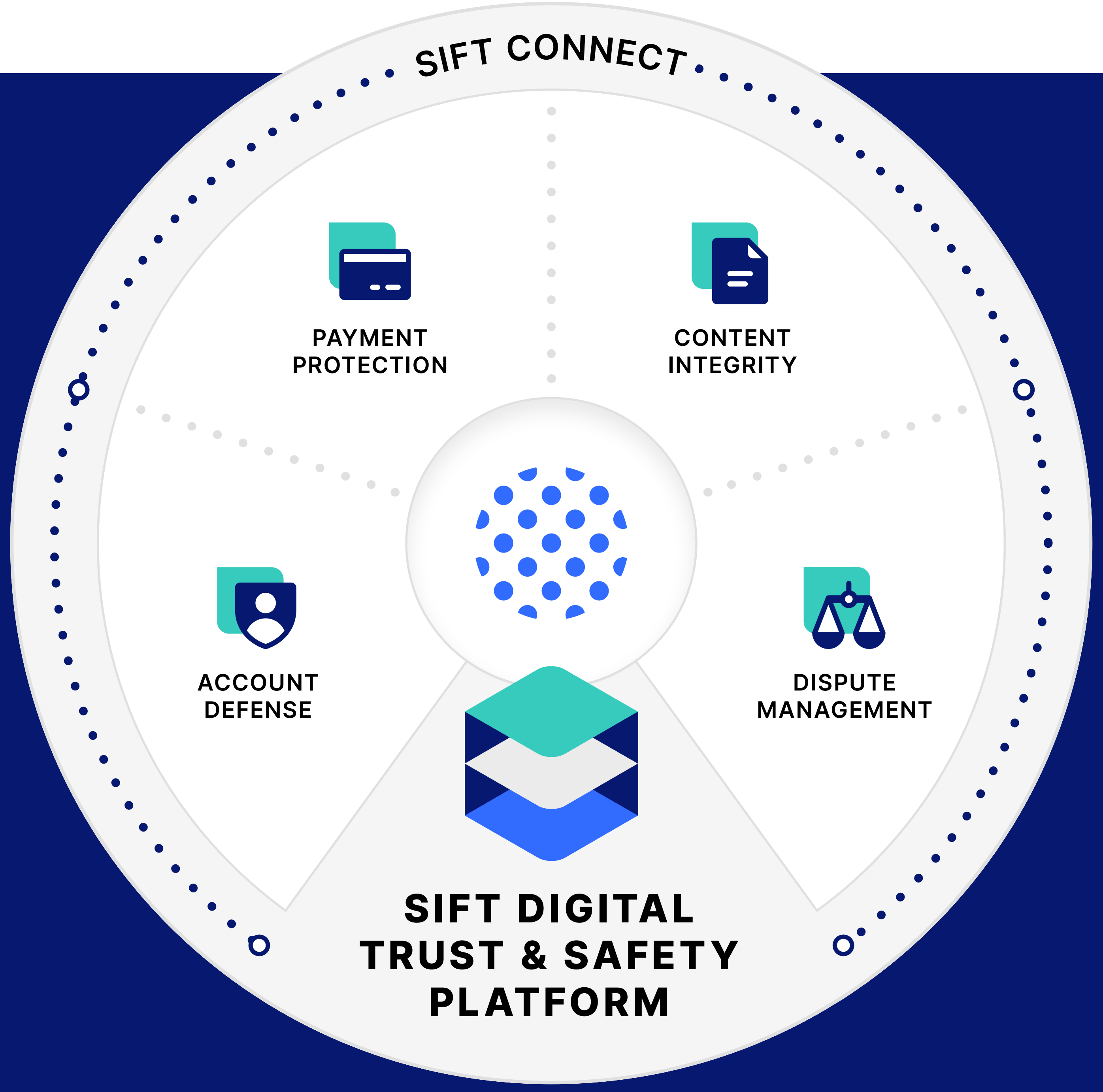
Businesses need the right tools to successfully stop account takeover fraud and prevent downstream payment abuse at scale. Sift's Digital Trust & Safety Platform helps digital risk teams gain control over losses and transparency into operations, fueling faster revenue growth with every transaction.

Our award-winning Account Defense product is purpose-built to help businesses of every size automatically prevent and stop large-scale bot-based account attacks with automated risk decisioning.

Account Defense allows analysts to instantly identify account takeovers at login with intelligent automation powered by real-time machine learning. Businesses can deliver frictionless experiences to trusted users and kick risky sessions to review, protecting every user with automatic customer notifications in response to suspicious activity.

Automated risk decisions with Sift Workflows let trust and safety teams deep-dive into complex cases, and accelerate manual review with a comprehensive view into account activity and data using the intuitive, customizable Sift Console. Take our Digital Trust & Safety Assessment today to discover how Sift can protect your business from checkout to chargeback.

The data highlighted in this report is derived from Sift's global data network of one trillion (1T) events, and compares findings from Q2 2022 to Q2 2023. This report also includes insights gathered on behalf of Sift by Researchscape, which polled 1,035 U.S. adults (aged 18+) in July of 2023.



Companies that adopt an end-to-end, real-time approach, backed by a network of global fraud signals and events, improve fraud detection accuracy by 40%.

Learn more at sift.com →

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 1 trillion (1T) annual events. Global brands including **DoorDash**, Blockchain.com, and **Paula's Choice** rely on Sift to catalyze growth and stop fraud before it starts. Visit us at **sift.com**, or follow us on **LinkedIn**.