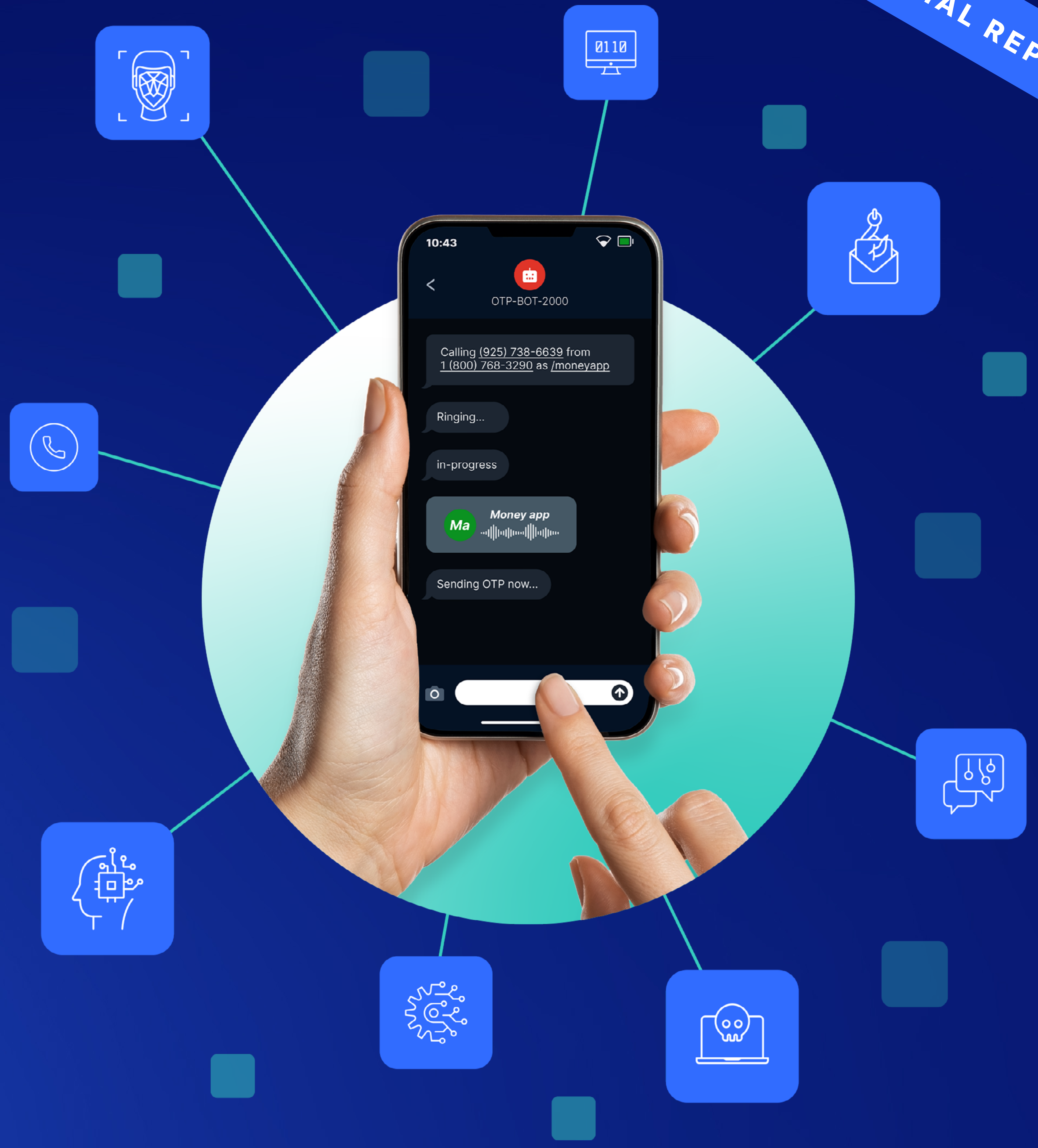
SPECIAL REPORT

sift

Q2 2023 DIGITAL TRUST & SAFETY INDEX

Fighting fraud in the age of AI and automation



10:43

OTP-BOT-2000

Calling (925) 738-6639 from 1 (800) 768-3290 as /moneyapp

Ringing...

in-progress

Ma Money app

Sending OTP now...

Contents

THE EVOLUTION OF FRAUD

AI and automation are changing the scope of fraud

Generative artificial intelligence (AI) has changed the internet as we know it. The breakthrough technology, powering popular chatbots like ChatGPT and Bard, uses algorithms to generate original content in the form of text, code, images, audio, and video based on virtually any given prompt.

ChatGPT recently surpassed 1 billion users, gaining immediate attention from consumers and media worldwide. But the breakthrough technology is proving to be a double-edged sword. While earning praise for its creative potential, generative AI is also under intense scrutiny for the serious risk it poses.

The result is a virtual arms race between leading tech giants to win market share using the power of artificial intelligence—and among fraudsters, hellbent on exploiting its impressive functionality. AI's capacity to disrupt is only beginning to take shape, and merchants that don't acknowledge the shift will be unable to survive it.

Consumers are paying close attention to the perks of tools like ChatGPT, but are also expressing concern over the potential threat to their jobs and increasingly convincing scams. More than **three in four** consumers said they're worried AI will be used to defraud them.

78%

of consumers are concerned about AI being used to defraud them

The data shows there's reason to be concerned. In the last six months, **68%** of consumers noticed an increase in the frequency of spam and scams, likely driven by the surge in AI-generated content. And Sift data shows a **40%** increase in the average rate of fraudulent content blocked from the network in Q1 2023 vs. the entirety of 2022. This trajectory is only expected to continue.

Spam and scams are on the rise in 2023

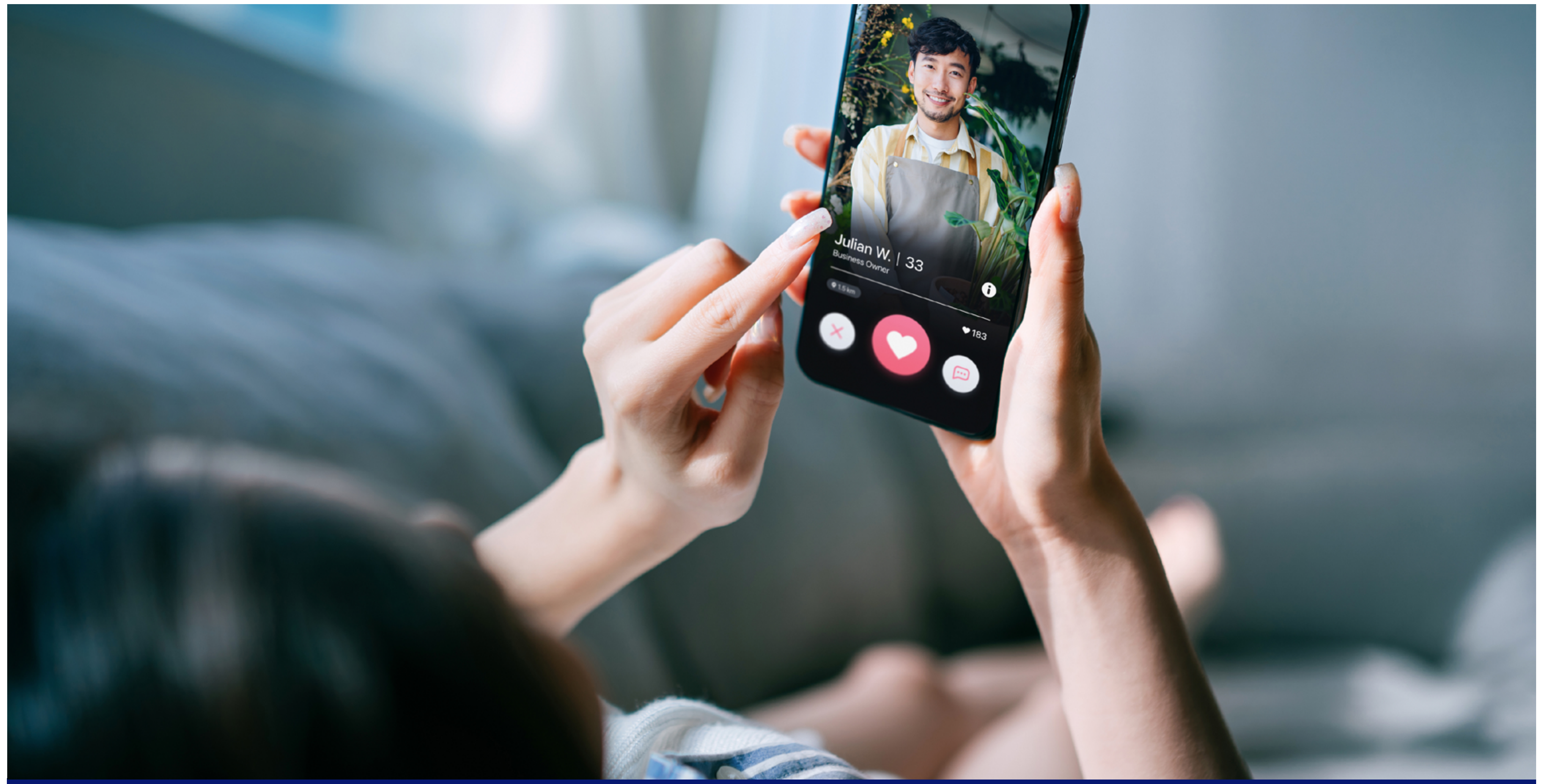
68%
of consumers noticed an increase in the frequency of spam and scams in the last six months

40%
increase in the average rate of fraudulent content blocked by Sift in Q1 2023 vs. all of 2022

Generative AI is proving to be a game changer for fraudsters. Its ability to create conversational language free of spelling, grammatical, or verb tense errors makes it difficult for the average person to distinguish this “synthetic media” from the authentic.

This is creating a flood of disinformation and scams. And it’s no longer a matter of shutting down individual bad actors. When AI technology is available to anyone, its uses are nearly limitless. Tools like ChatGPT represent an endless network that benefits from instant knowledge-sharing capable of doing the work of humans at an entirely inhuman speed.

These advancements in AI are helping fraudsters launch more convincing scams with **social engineering** by tricking people into revealing confidential information, including account credentials and payment details. Recent AI voice scams, for example, use online voice replication tools to impersonate victims’ loved ones in distress, which have swindled people out of thousands of dollars.



What is social engineering?

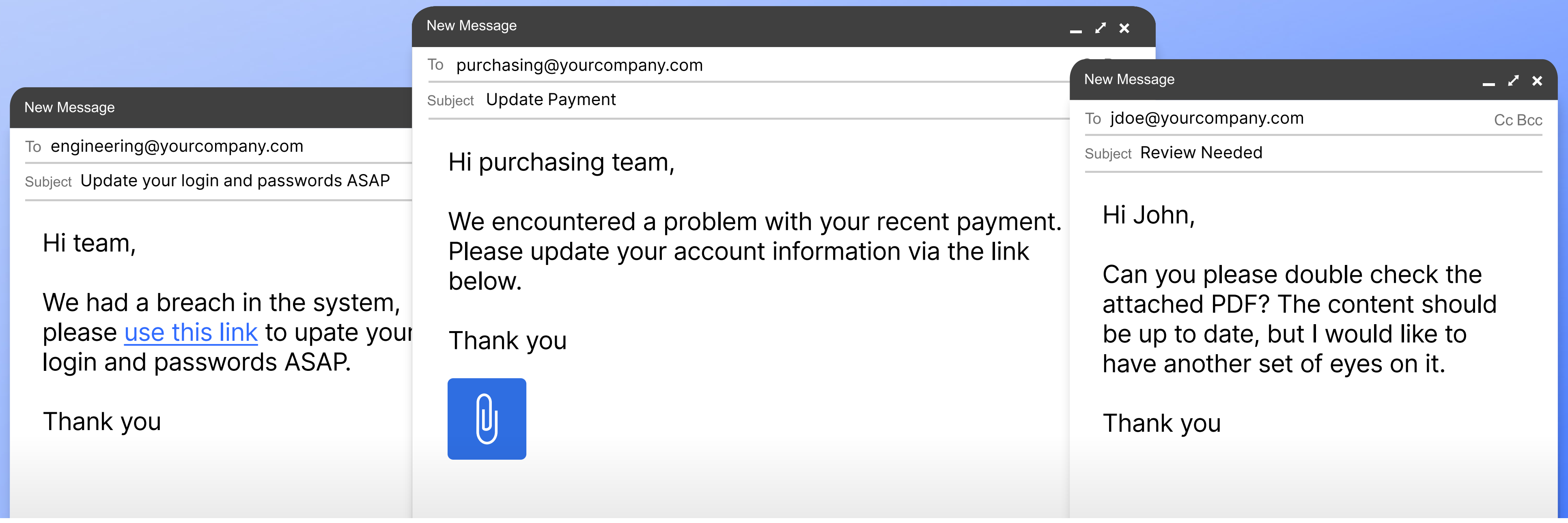
Social engineering is a scam tactic that involves a fraudster impersonating another trusted individual or company in order to deceive them into sharing confidential credentials or payment information. These scams can take place via phone calls, texts, email, social media sites, dating apps, and other websites. Nearly all cybercrime (98%) involves social engineering, making it the most common abuse tactic used globally by fraudsters.

In 2022, consumers reported losing $2.6 billion to imposter scams, with those executed over social media and phone calls leading to the highest losses. This increase in social engineering scams is leading to a jump in downstream fraud, including account takeovers (ATO) and eventually payment fraud.

Once a fraudster is able to successfully phish account credentials and/or payment information, they'll use it to access the victim's accounts and make unauthorized purchases. In the first quarter of 2023, the rate of account takeover attacks rose a staggering **427%** compared to all of 2022.

The surging threat of business email compromise

Business email compromise (BEC) is a type of scam in which fraudsters lure employees into opening malicious emails and providing login credentials or banking information. It's one of the most financially damaging social engineering threats, rising 81% in 2022 and costing companies $43 billion in recent years. The emergence of AI-generated emails impersonating executives, coupled with employees' poor password hygiene and low reporting rates, make these scams a significant—and fast-growing—risk for businesses.



New Message

To engineering@yourcompany.com

Subject Update your login and passwords ASAP

Hi team,

We had a breach in the system, please use this link to upate your login and passwords ASAP.

Thank you

New Message

To purchasing@yourcompany.com

Subject Update Payment

Hi purchasing team,

We encountered a problem with your recent payment. Please update your account information via the link below.

Thank you

New Message

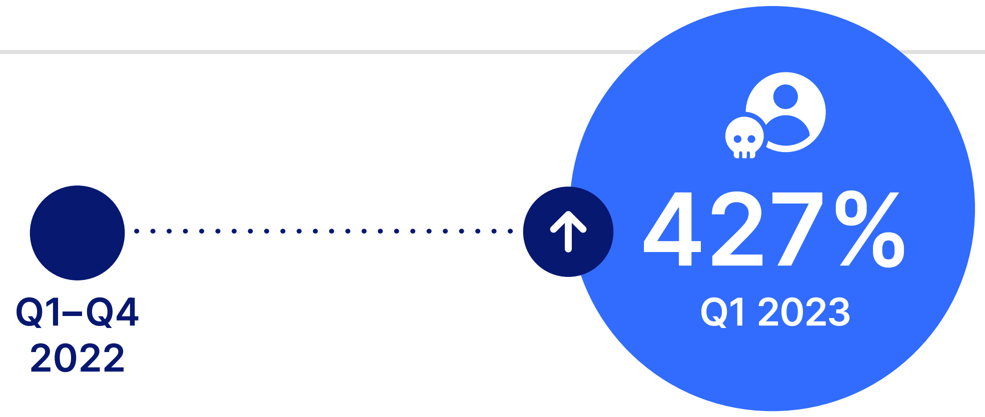
To jdoe@yourcompany.com Cc Bcc

Subject Review Needed

Hi John,

Can you please double check the attached PDF? The content should be up to date, but I would like to have another set of eyes on it.

Thank you

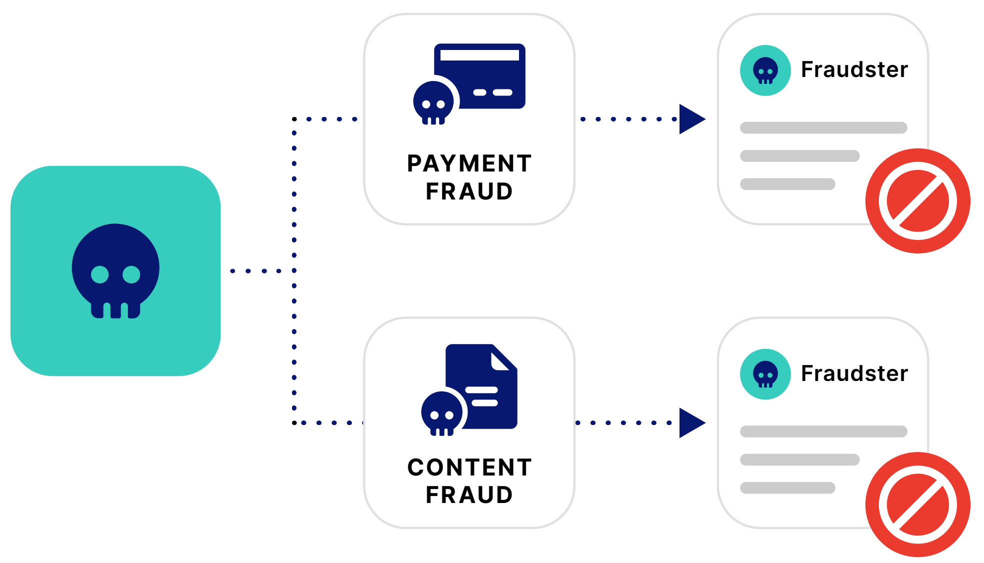


The rate of blocked account takeovers jumped 427% in Q1 2023 vs. all of 2022

This massive spike in ATO can be partially attributed to the AI-enhanced social engineering attacks driven by automation, including one-time password (OTP) bots, scraper bots, and automated phishing attacks. The security of ChatGPT itself has also come under fire, after OpenAI confirmed a recent data breach, which exposed users' contact information and partial payment information.

We're now watching a perfect storm for fraud unfold, with the accuracy and believability of AI-generated content being paired with the rapid-fire speed of automation. This is evident across the Sift network, with blocked content and blocked payments from the same fraudster increasing **66%** from Q4 2022–Q1 2023 compared to Q2–Q3 2022. The same bad actors are increasingly approaching fraud from multiple angles to rapidly test platforms for weaknesses. By automating these tactics, fraudsters can buy themselves more time to diversify their attack vectors and maximize their chances for success.

Estimates show fraud will likely keep escalating in the years to come. Global e-commerce fraud loss is estimated to reach $48 billion by the end of 2023, a 16% YoY increase. And between 2023 and 2027, the cumulative merchant losses to online payment fraud are expected to exceed $343 billion.



↑66%

increase in blocked content and blocked payments from the same fraudster Q4 2022–Q1 2023 vs. Q2–Q3 2022

ADVANCING TACTICS AND TECHNOLOGY

Fraudsters are strengthening their attacks

Fraudsters are starting to overcome the vulnerabilities that typically expose their social engineering scams, such as typos, grammatical errors, and unusual cadence or phrasing. By leveraging generative AI, they can create more convincing, automated social engineering attacks that remove clear giveaways. With the help of these tools, fraudsters can rapidly advance their strategies and tactics before businesses can respond.

AI-generated content allows fraudsters to not only eliminate bad spelling and grammatical errors in English, but commit better fraud attacks in various languages as well. These AI tools can also write and improve code, removing telltale signs of bot activity. It can even suggest variations of text that allow a fraudster to spin up multiple accounts on a platform without them seeming too similar. For example, they can create 100 new dating profiles to commit Pig Butchering scams, each with a unique AI-generated face and bio.

Although nearly **80%** of consumers feel confident they could identify a scam generated by AI, the reality is that ongoing advancements in this technology are making it increasingly difficult to do so. **Nearly half** of consumers admit it's become more difficult to identify scams in the past 6 months, about as long as ChatGPT has been available. In fact, research shows people are 10% more likely to click links that are generated by AI.

Scams get trickier to spot

49% of consumers say it's become harder to identify scams in the last 6 months

21% of consumers don't feel confident they could identify a scam created by AI

> “
>
> Much like the disruption and innovation that calculators introduced to math classrooms, breakthroughs in AI will make it easier and faster for criminals to create fraudulent content—and the scale will extend well beyond what we currently see.

Brittany Allen
Trust and Safety Architect at Sift

The democratization of fraud gets automated

As technology advances, fraud evolves along with it. It’s easy for anyone to become a fraudster and scale attacks with speed, even with minimal experience. This furthers the democratization of fraud, allowing anyone with malicious intent to participate in nefarious activity online.

Rapid developments in AI and automation, paired with easily-accessible forums on the deep web, open the doors for even those without technical expertise or fraud knowledge to cash in. More experienced cybercriminals are capitalizing on this by turning their fraud skills into on-demand services for sale, known as fraud-as-a-service (FaaS).

Recently, Sift trust and safety experts have observed an influx of FaaS schemes centered around automation and bots, particularly bots using one-time password (OTP) SMS. Bots make up nearly two-thirds of internet traffic, with bad bots accounting for nearly 40% of all traffic—a number that continues to rise. Last year alone, bad bot traffic rose 102% YoY, even as legitimate human traffic declined.

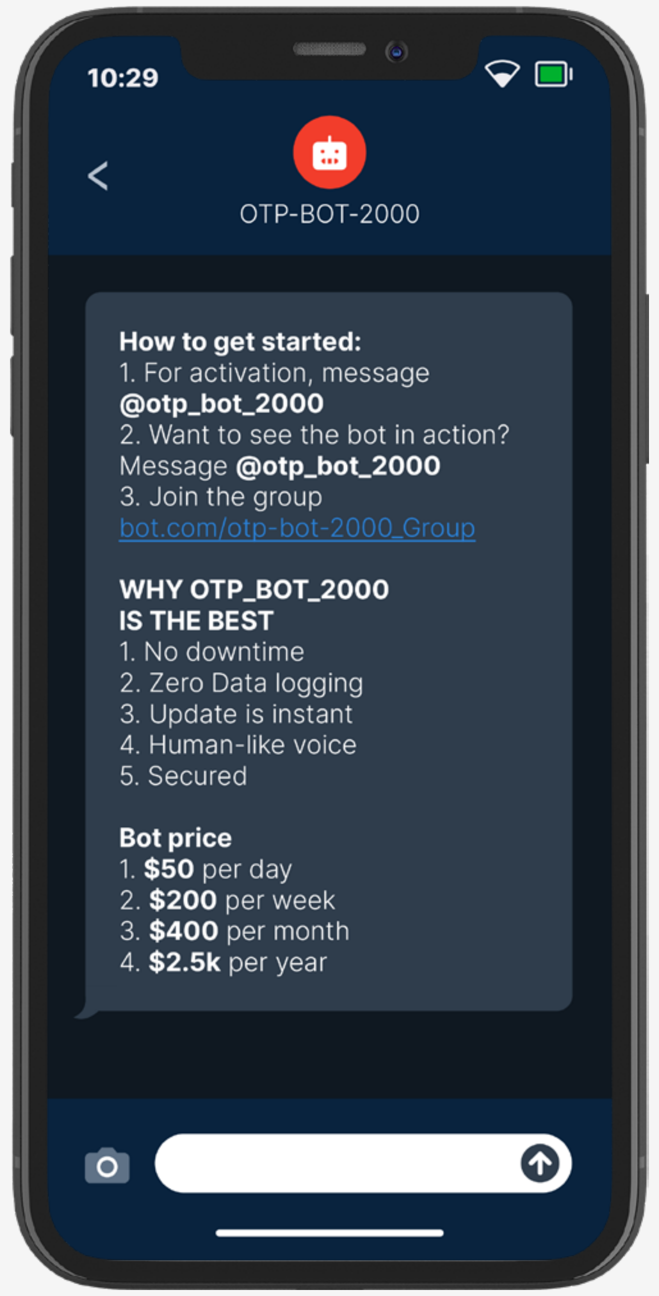
One such bot-as-a-service scam operates through encrypted messaging apps like Telegram and is used to obtain OTP SMS codes from victims. The bot works by spoofing a company or financial institution’s caller ID to trick victims into providing their OTPs for anything from bank logins to payment service apps. Fraudsters can pay for use of the bot on a daily, weekly, monthly, or yearly basis. And while most won’t fall for these scams, the scalability of bots make it a profitable numbers game for fraudsters.

sift

BOTS-AS-A-SERVICE

Mechanics of an automated scam

STEP 1


10:29

OTP-BOT-2000

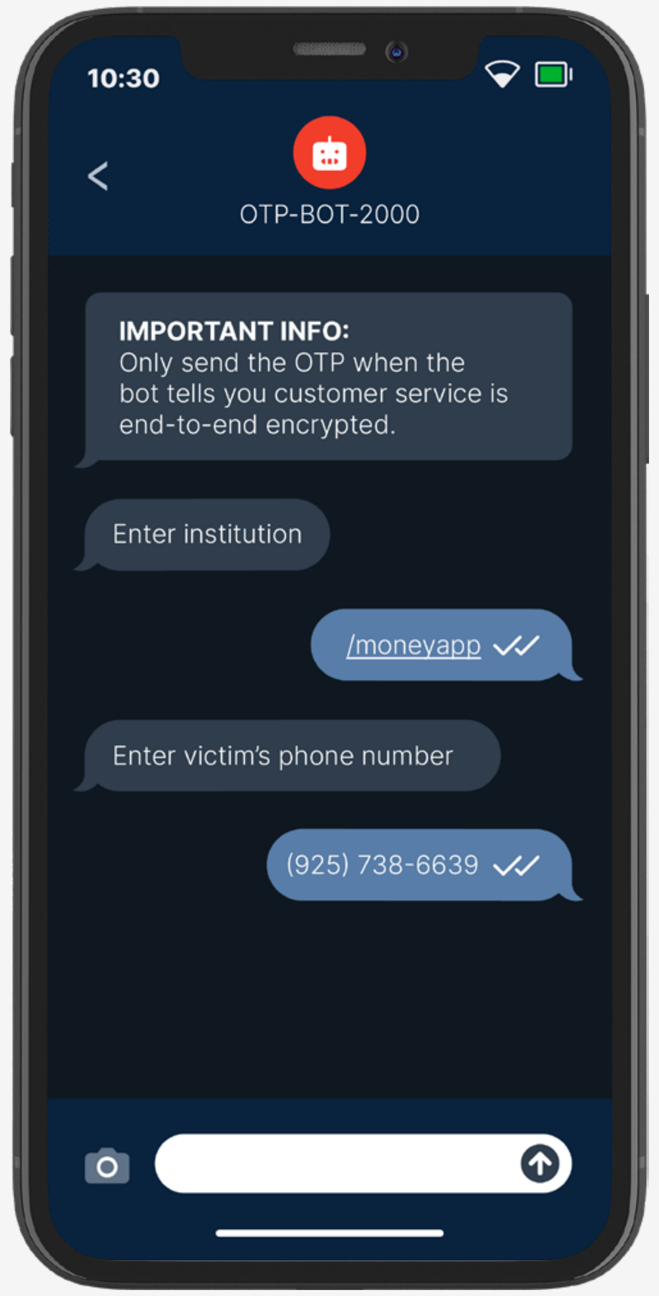
How to get started:
1. For activation, message
@otp_bot_2000
2. Want to see the bot in action?
Message **@otp_bot_2000**
3. Join the group
bot.com/otp-bot-2000_Group

WHY OTP_BOT_2000
IS THE BEST
1. No downtime
2. Zero Data logging
3. Update is instant
4. Human-like voice
5. Secured

Bot price
1. **$50** per day
2. **$200** per week
3. **$400** per month
4. **$2.5k** per year

The fraudster joins a scam group on a deep web forum and pays for use of the OTP bot.

STEP 2


10:30

OTP-BOT-2000

IMPORTANT INFO:
Only send the OTP when the bot tells you customer service is end-to-end encrypted.

Enter institution

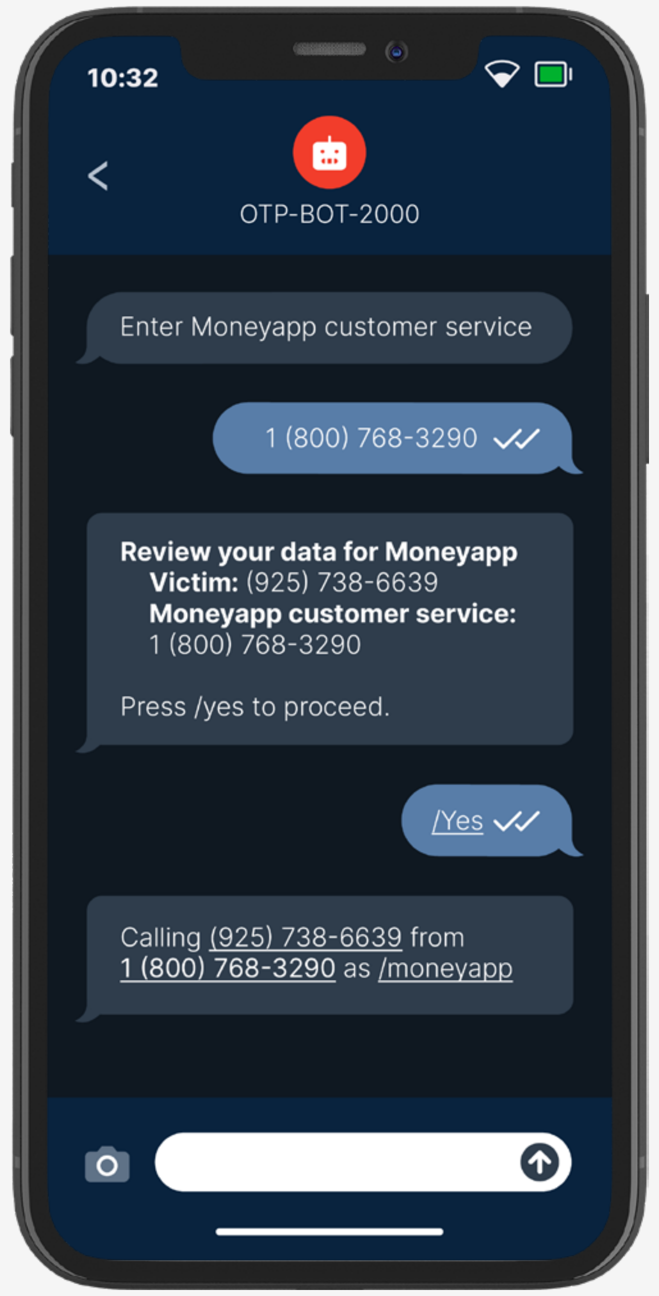
/moneyapp ✓✓

Enter victim's phone number

(925) 738-6639 ✓✓

The fraudster enters the victim's phone number into the OTP bot.

STEP 3


10:32

OTP-BOT-2000

Enter Moneyapp customer service

1 (800) 768-3290 ✓✓

Review your data for Moneyapp
Victim: (925) 738-6639
Moneyapp customer service:
1 (800) 768-3290

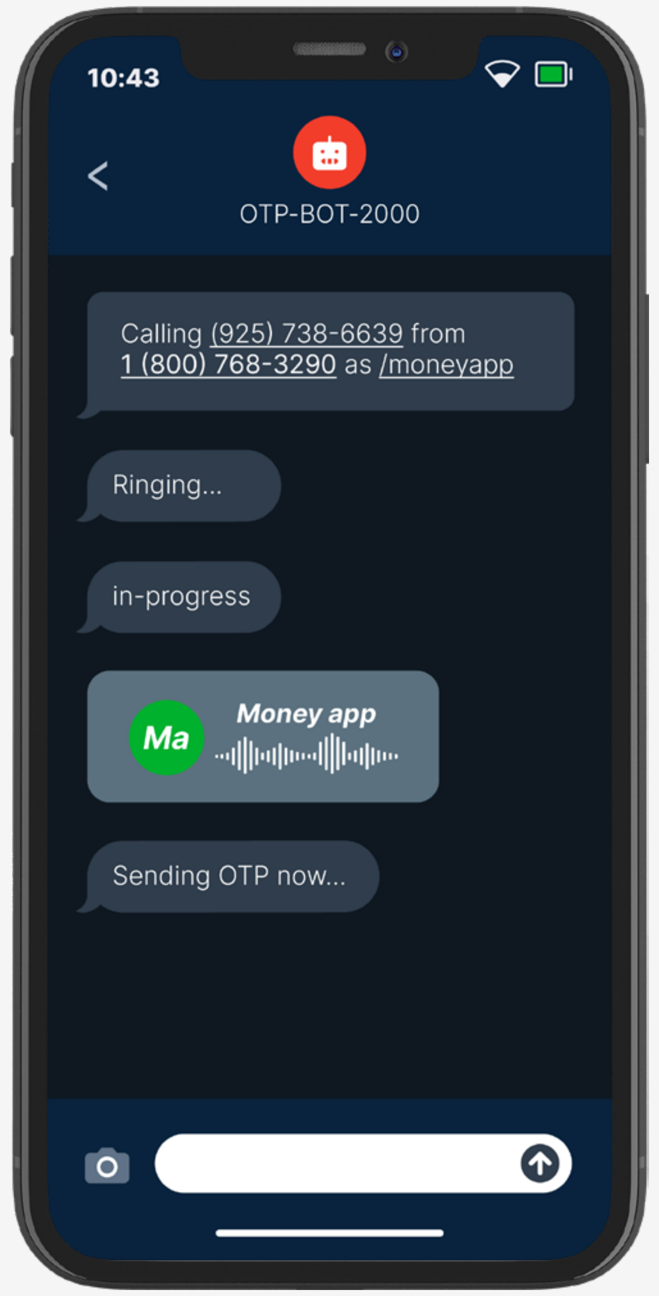
Press /yes to proceed.

/Yes ✓✓

Calling (925) 738-6639 from
1 (800) 768-3290 as /moneyapp

The fraudster provides the bot with the caller ID for the site or app they want to spoof.

STEP 4


10:43

OTP-BOT-2000

Calling (925) 738-6639 from
1 (800) 768-3290 as /moneyapp

Ringing...

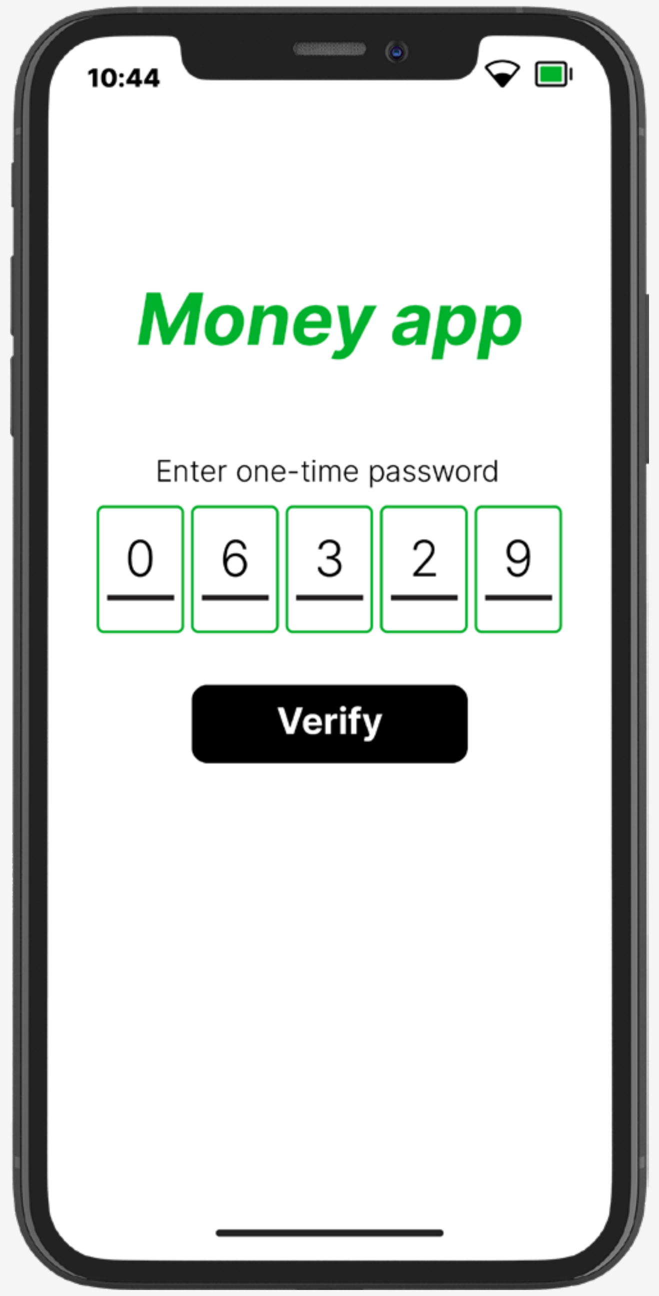
in-progress

Ma *Money app*

Sending OTP now...

The bot calls or texts the victim, impersonates the business, and asks them to provide their OTP.

STEP 5


10:44

Money app

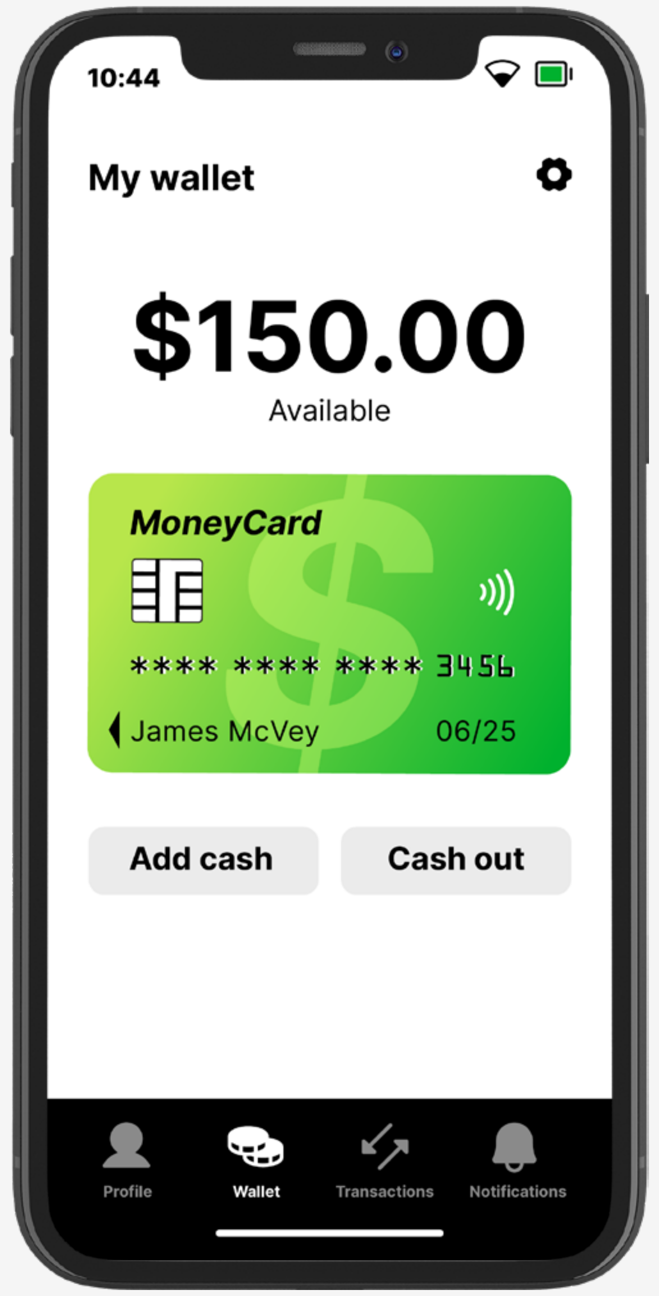
Enter one-time password

0 6 3 2 9

Verify

The fraudster receives the OTP to successfully log into the victim's account.

STEP 6


10:44

My wallet

$150.00
Available

MoneyCard
**** **** **** 3456
James McVey 06/25

Add cash | Cash out

The fraudster can now steal the victim's payment info to make unauthorized purchases.

Consumers are falling victim to fakeouts

The full potential of generative AI is unknown, but it's inevitable that it will be leveraged throughout the Fraud Economy. Cybercriminals will continue to develop their tactics, overwhelming the internet with various shapes of social engineering scams that will result in an influx of downstream fraud.

As AI improves social engineering attacks, it's leading to increasingly successful account takeovers, ultimately with the intention of draining stored value in those accounts or committing financial fraud with on-file payment information. According to consumers, in the last 6 months **nearly 20%** of them have been successfully phished, and **17%** of them have been a victim of ATO or payment fraud. These numbers are likely to increase as fraudsters find new ways to exploit AI and automation for malicious use.

Consumers get phished, ATO'd, and defrauded

19%
of consumers indicate that they've been successfully phished in the last 6 months

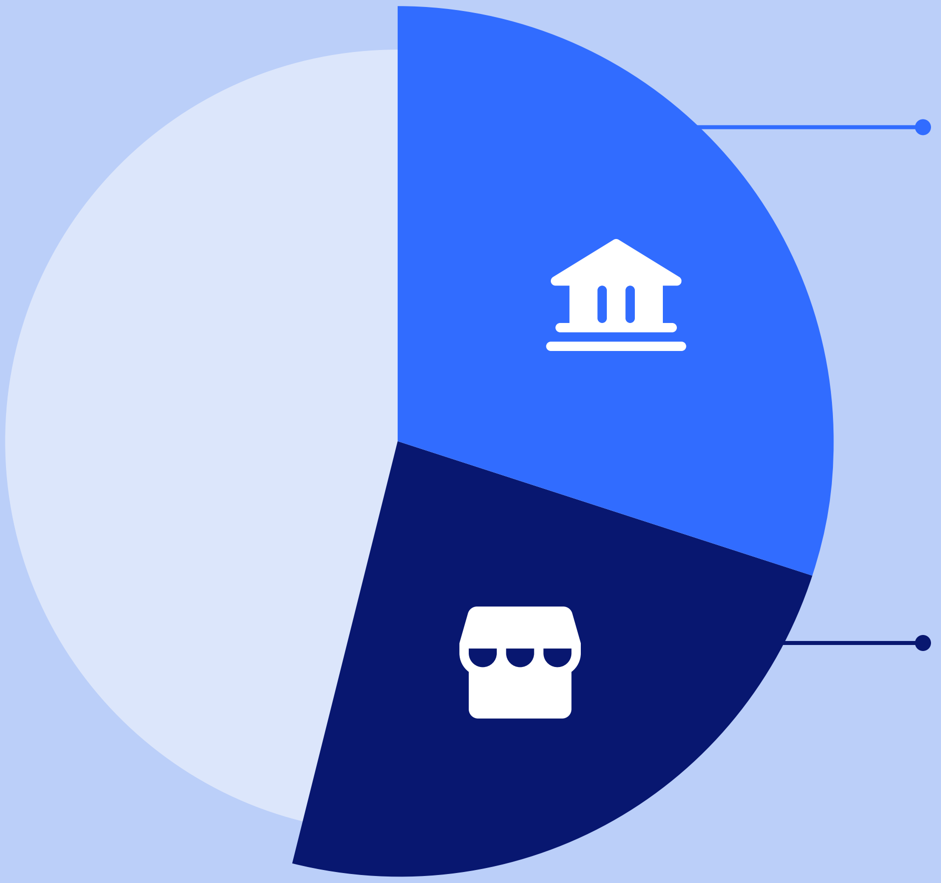
17%
of consumers have been a victim of ATO or payment fraud in the last 6 months

The rise of deep fakes

Fraudsters are increasingly using generative AI to create strikingly accurate deep fake videos and voice clones to facilitate imposter scams and financial fraud.

30% of consumers believe someone has tried to defraud them using a deep fake

54% of consumers believe they shouldn't be held responsible if they were scammed into providing their payment information and it was then used to make an unauthorized purchase



30%
believe their bank or financial institution is responsible

24%
believe the business where the attempted purchase was made is responsible

RISK MANAGEMENT STRATEGIES

Businesses can take control with proactive fraud prevention

As long as there's valuable data to be stolen, fraudsters will find ways to abuse new technologies, using them to break through fraud and security controls. AI regulations could be on the horizon, with lawmakers around the world in the process of negotiating guardrails for AI chatbots, including an AI bill of rights and even strict censorship rules. But for now, **it's up to companies to set standards on their own platforms in order to keep their business and customers safe from the downstream effects of AI-based fraud attacks.**

More than half of consumers (54%) believe they shouldn't be held responsible in the event they unintentionally provided their payment information to a scammer that was later used to make a fraudulent purchase. Of those 54%, **30%** believe their bank or financial institution should be responsible for preventing the fraudulent transaction, while **24%** believe it should be on the business where the attempted purchase was made.

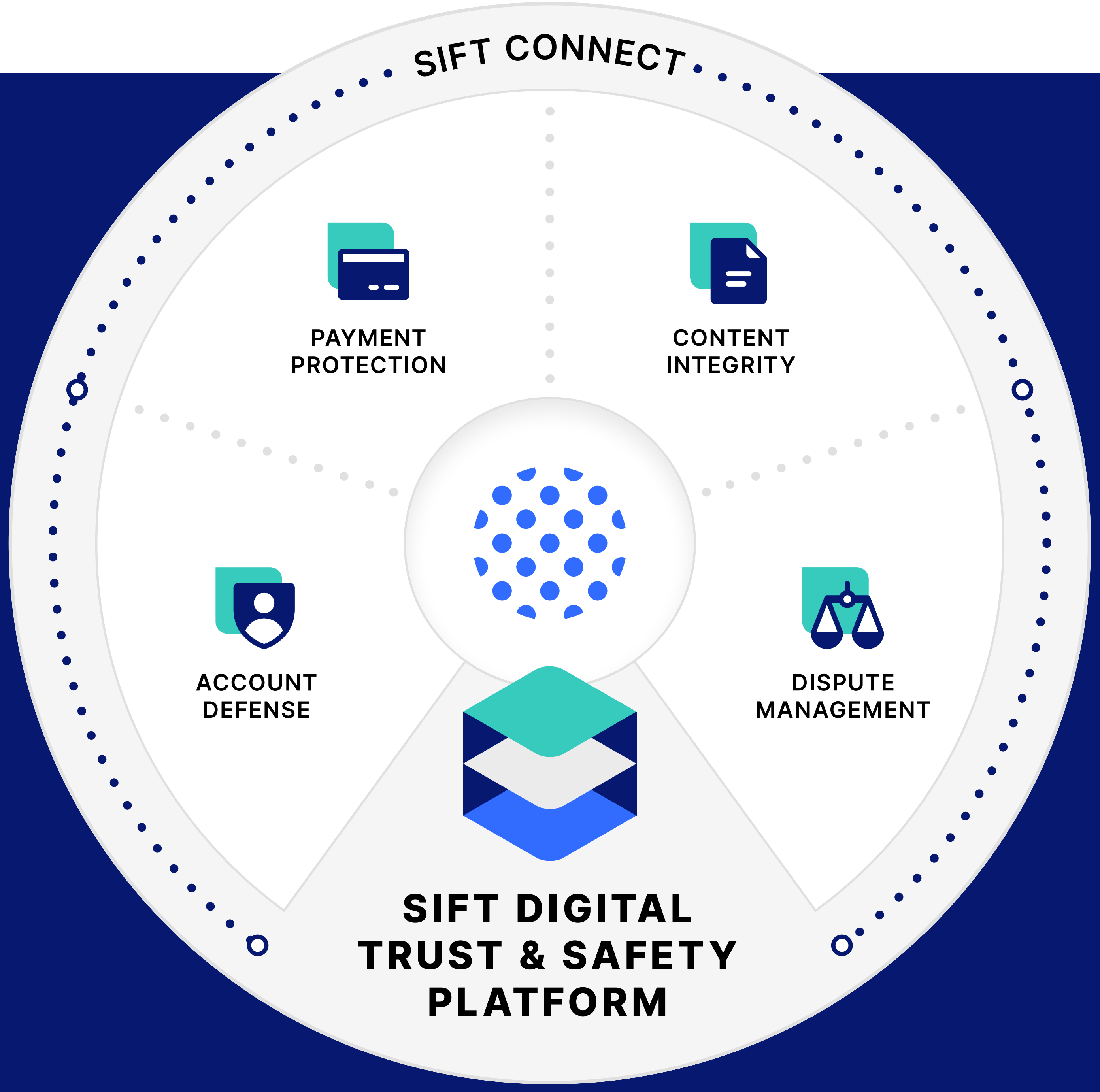
> “
>
> Real-time ML is crucial to keep up with the scale, speed, and sophistication of fraud. Merchants who don’t move away from manual review will fall behind fraudsters who are already automating. ML helps us identify patterns that we cannot yet predict for AI-empowered fraud.
>
>
>
> **Brittany Allen**
> **Trust and Safety Architect at Sift**

Strong defenses and a future-forward fraud strategy can help prevent the threat of AI and bot-fueled ATO and payment fraud. Businesses that only focus on a few known red flags won’t be able to keep up with evolving risk. Instead, they must look at transactions holistically to differentiate between fraudulent and legitimate activity.

Businesses need a comprehensive, real-time solution to keep up with fraudsters who are leveraging more dangerous and easily-accessible tools. Sift helps protect businesses from malicious bot use by combining bot detection with the flagship Digital Trust & Safety Platform to prevent automated attacks.

Analysts need the right tools to successfully prevent fraud and optimize operations to enable revenue growth. **Take our Digital Trust & Safety assessment to get customized insights and recommendations for your business.**

**The data highlighted in this report is derived from Sift’s global data network of one trillion (1T) events across 2022 and 2023, along with insights gathered on behalf of Sift by Researchscape, which polled 1,091 U.S. consumers (aged 18+) in April 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 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, Poshmark, and Twitter rely on Sift to gain a competitive advantage in their markets. Visit us at **sift.com**, and follow us on **LinkedIn**.