

Identity Fraud in Focus Quarterly Report

JANUARY - MARCH 2023



With Identity Fraud in Focus, we leverage our research and internal fraud data to provide insights so experts, organizations and consumers can stay informed about emerging threats online.

KEY DISCOVERIES

✓ Top identity theft and fraud crimes from Q1

✓ ChatGPT, AI, and emerging digital threats

AllstateSM
IDENTITY PROTECTION

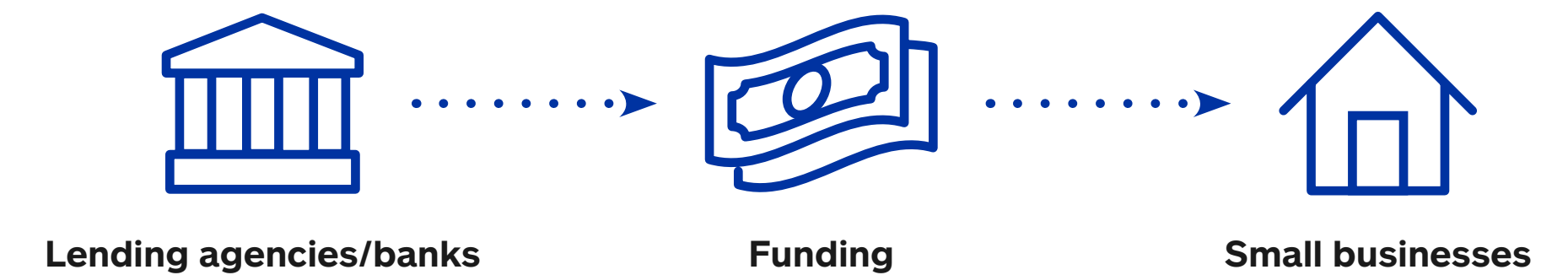


top identity theft and fraud crimes from Q1

Small Business Administration (SBA) Fraud

How the SBA works

The SBA works with lending agencies and banks to make it easier for small businesses to obtain loans. During the COVID-19 pandemic, SBA also provided direct funding to small businesses through grants, disaster loans, and economic stimulus programs, such as the Paycheck Protection Program (PPP).



SBA-related fraud and the pandemic

In total, the federal government provided approximately \$4.6 trillion to help the nation recover from the COVID-19 pandemic.¹ Unfortunately, bad actors took advantage of loopholes in the system to steal billions in taxpayer money.

While no one is sure how much was stolen, conservative estimates suggest the PPP program alone was looted for nearly \$80 billion in what former U.S. attorney Matthew Schneider calls “the biggest fraud in a generation.”²

That’s on top of the \$90-\$400 billion stolen from jobless relief programs (i.e. unemployment and disability fraud) during the peak of the pandemic, as well as another \$80 billion potentially embezzled from a separate Covid relief fraud.²

QUICK TAKEAWAYS

\$80 billion

— the estimated amount stolen from the PPP loan program²

213%

the increase in SBA New Account Fraud in the first quarter of 2023³

Sources:

- 1: U.S. Government Accountability Office, “COVID-19 Relief: Funding and Spending as of Jan. 31, 2023,” February 28, 2023.
- 2: NBC News, “Biggest fraud in a generation”: The looting of the Covid relief plan known as PPP,” March 28, 2022.
3. Allstate Identity Protection, Internal Restoration Stats, Q1 2023



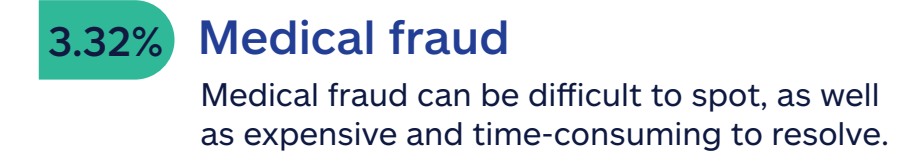
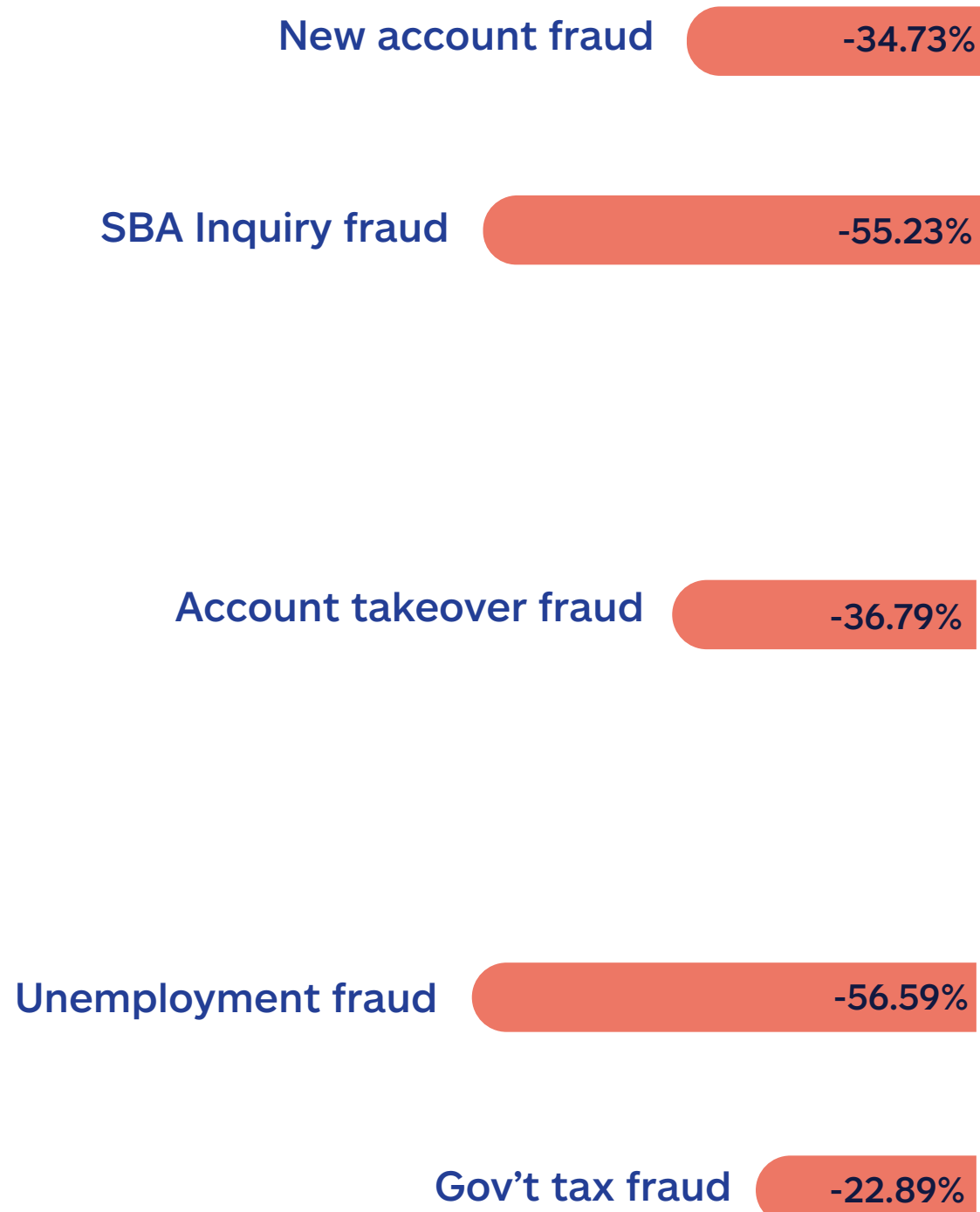
What is happening now with SBA loan fraud

We've been tracking Covid-19 identity fraud since the beginning of the pandemic, but the effect on individual victims will take years to untangle, which is why SBA new account fraud saw the highest increase of any fraud type in the first quarter of 2023, three years after the pandemic began.



“SBA loans fraudulently taken out during the pandemic are now coming due,” says Allstate Identity Protection Restoration Manager Vera Tolmachoff, “and victims are receiving letters from the SBA asking for repayment. If you receive a verified letter from the SBA for a loan you didn't take out, then follow their directions to a T. If you're a member and have been the victim of identity theft, contact us immediately. We're working with members to provide the necessary documents so the SBA can resolve their fraud cases.”

Q1 YoY growth*



*normalized to account for total subscriber growth

Sources:
Allstate Identity Protection, Internal Restoration Stats, Q1 2023

new artificial intelligence software is being exploited by scammers

ChatGPT, OpenAI's artificial intelligence chatbot, amassed over 100 million users in its first two months, making it the fastest-growing app in history.⁵ The language model can answer questions and assist with basic online tasks such as writing emails, essays, and source code with accuracy and precision. Uploaded information is stored by the software and helps the model learn. ChatGPT has the potential to help companies improve efficiency, reduce costs, and increase customer engagement, though the stored information could create some privacy risk.

Like any new technology that takes the internet by storm, scammers are

finding ways to cash in. In one scenario, fraudsters created a spoofed platform that promised free access to premium ChatGPT, which sells for \$20/mo on the official OpenAI site, with the goal to trick users into installing malware. Once downloaded from the app store, the malware can aid identity fraud by stealing stored data in users' applications, such as passwords or credit card info, and send it back to the hacker.⁶

Another spoofed site installed "chatGPT1," which secretly subscribed victims to numerous paid services without their knowledge or consent in what's commonly known as SMS billing fraud.⁶ Cybersecurity leader Bitdefender recently

warned about another scam that uses a spoofed ChatGPT platform to swindle eager investors. Targets were sent an unsolicited email "luring users with financial opportunities that pay up to \$10,000 per month." After clicking on the link and a brief exchange with a chatbot, the fraudsters asked for a contact number. Then, ten minutes later, the scam target received a call offering the chance to invest in "crypto, oil, and international stock." This was an attempt to steal personal and financial info.⁷

 [Click for additional tips](#)



KEY TAKEAWAYS

100M+

users of ChatGPT in its first two months, making it the fastest-growing app in history.⁴

Sources:

4: Time, "How ChatGPT Managed to Grow Faster than TikTok or Instagram," February 8, 2023.

5: Bleeping Computer, "Hackers use fake ChatGPT apps to push Windows, Android malware," February 22, 2023.

6: Mashable, "Scammers are spoofing ChatGPT to spread malware," February 23, 2023.

7: Bitdefender, "Bitdefender Labs warns of fresh phishing campaign that uses copycat ChatGPT platform to swindle eager investors," March 6, 2023.



"Scammers using the latest technology to defraud users is nothing new," says Robert Neel, Chief Information Security Officer at Allstate Identity Protection. "As with any functionality it is always safest to leverage the source. This means going to the OpenAI site to try ChatGPT, or ensure that you use the official mobile application. Stay away from unknown apps that may have integrated the technology or random links promising things leveraging ChatGPT."

about Identity Fraud in Focus

Providing insights from millions of identity theft cases since the start of 2021, Identity Fraud in Focus provides the knowledge families need to stay safer online.



“Now more than ever, people need extra information, guidance, and support to navigate today’s threats to their security and privacy — so they can keep their families safe,” says Dustin Hofstein, Chief Service Officer of Allstate Identity Protection. “That’s why our quarterly Identity Fraud in Focus report is so important, so consumers, experts, and the media understand the latest digital threats. And what people can do to live more secure lives.”

AllstateSM
IDENTITY PROTECTION