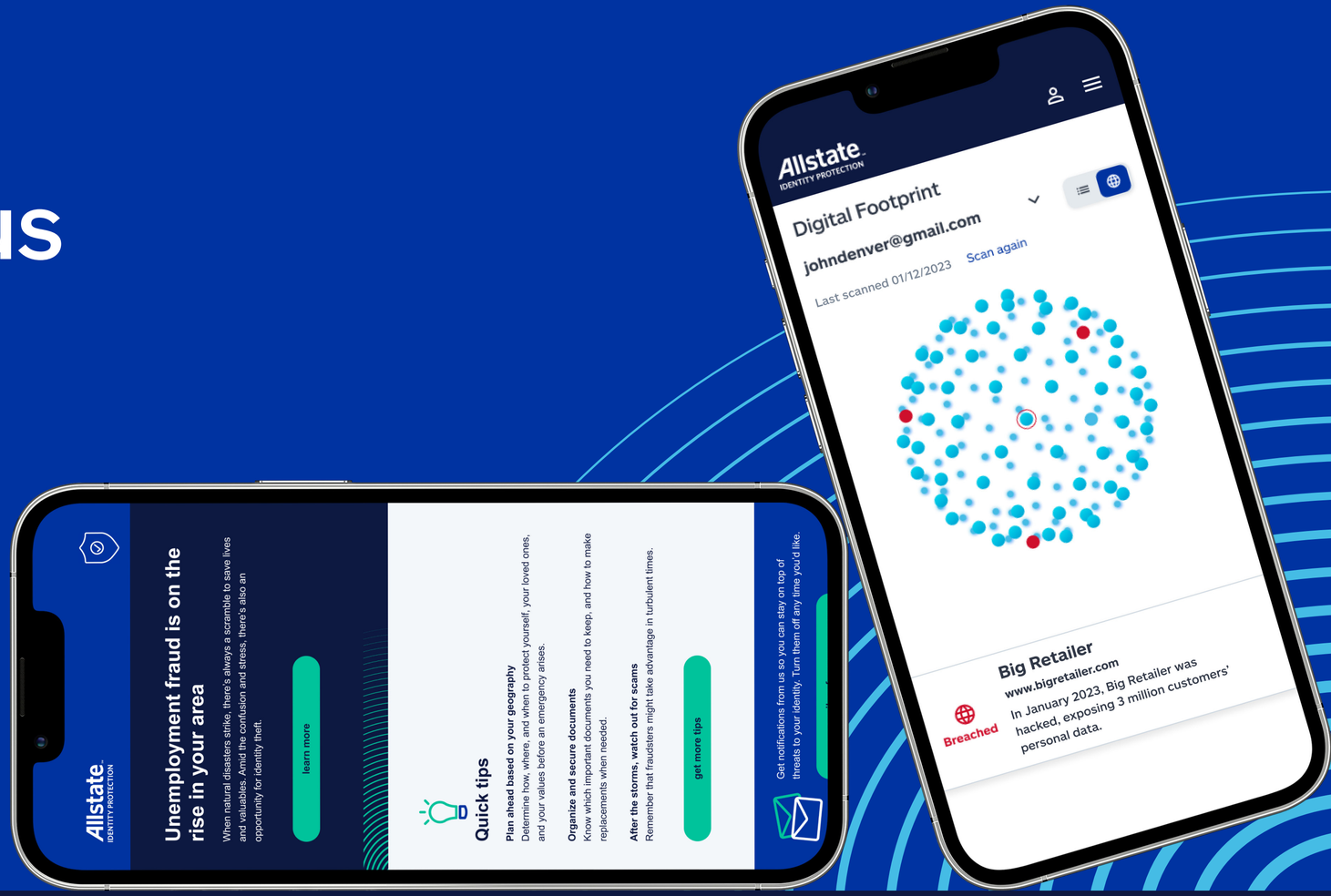
Identity Fraud in Focus Quarterly Report

APRIL - JUNE 2023



With this quarterly report, we leverage internal member data and research to give insight into emerging threats online for experts, organizations, and consumers.

KEY DISCOVERIES

- **Increase in reported unemployment fraud**
- **Data breaches hit a record pace**
- **Keep employees educated about the risks**

Allstate SM
IDENTITY PROTECTION

unemployment fraud, SBA new account fraud on the rise

SBA new account fraud up 200+% from Q1

Throughout spring 2023 we saw a continuing large spike — 204% — in the number of reports concerning SBA new account fraud. We previously reported a 213% increase in Q1 due to many types of loans and assistance from the pandemic coming due, thus notifying victims who may not have been aware.

Multiple quarters with triple digit increases in fraud reporting may not be cause for panic, but it does bear further monitoring — especially as student loan payments resume in October and consumers are potentially exposed to further fraud.

Unemployment fraud rises more than 22%

Unemployment fraud reports also rose in Q2 2023, counter to the U.S. unemployment rate decreasing slightly. According to the U.S. Government Accountability Office, an unprecedented need for benefits — spurred by the pandemic — paired with a rapid, sometimes chaotic implementation of new programs, led to blind spots and redundancy in some cases — fertile ground for fraudsters.

Medical fraud sees small increase

The rate of members reporting medical fraud rose by 5.8% from Q2 2022. Fraudsters can swipe insurance information through bogus marketing for “free” services as well as phishing attacks — as inflation pinches more families’ budgets, victims may fall for these offers and disclose their health or insurance information. Scammers have also posed as administrators seeking to help victims with settling medical debts — consumers might not think twice about reading their insurance card over the phone to someone offering to help with their medical billing.

KEY TAKEAWAYS

As inflation continues to pinch consumers and student debt loan payments resume (scheduled for October 2023), the need for financial aid programs like PPP, unemployment, and others will continue to rise. The COVID-19 pandemic may have subsided but the long-term effects as well as the risk of future variants could further strain healthcare systems.

Government agencies are tasked with balancing data security against making sure financial assistance programs are easily accessible and dispense payments quickly — as such we expect these types of fraud inquiry to continue increasing.

record-setting rate of data breaches

The Identity Theft Resource Center tracked 951 publicly-reported data compromises in Q2 alone — the highest number ever reported in a single quarter. The rate of data breaches so far in 2023 is on pace to set a new record.[1]

Nearly 50 million accounts were exposed in data breaches in the U.S. alone in Q2 2023 — part of a 156% increase in the number of accounts leaked from 2022, according to Netherlands-based VPN provider Surfshark.[2]

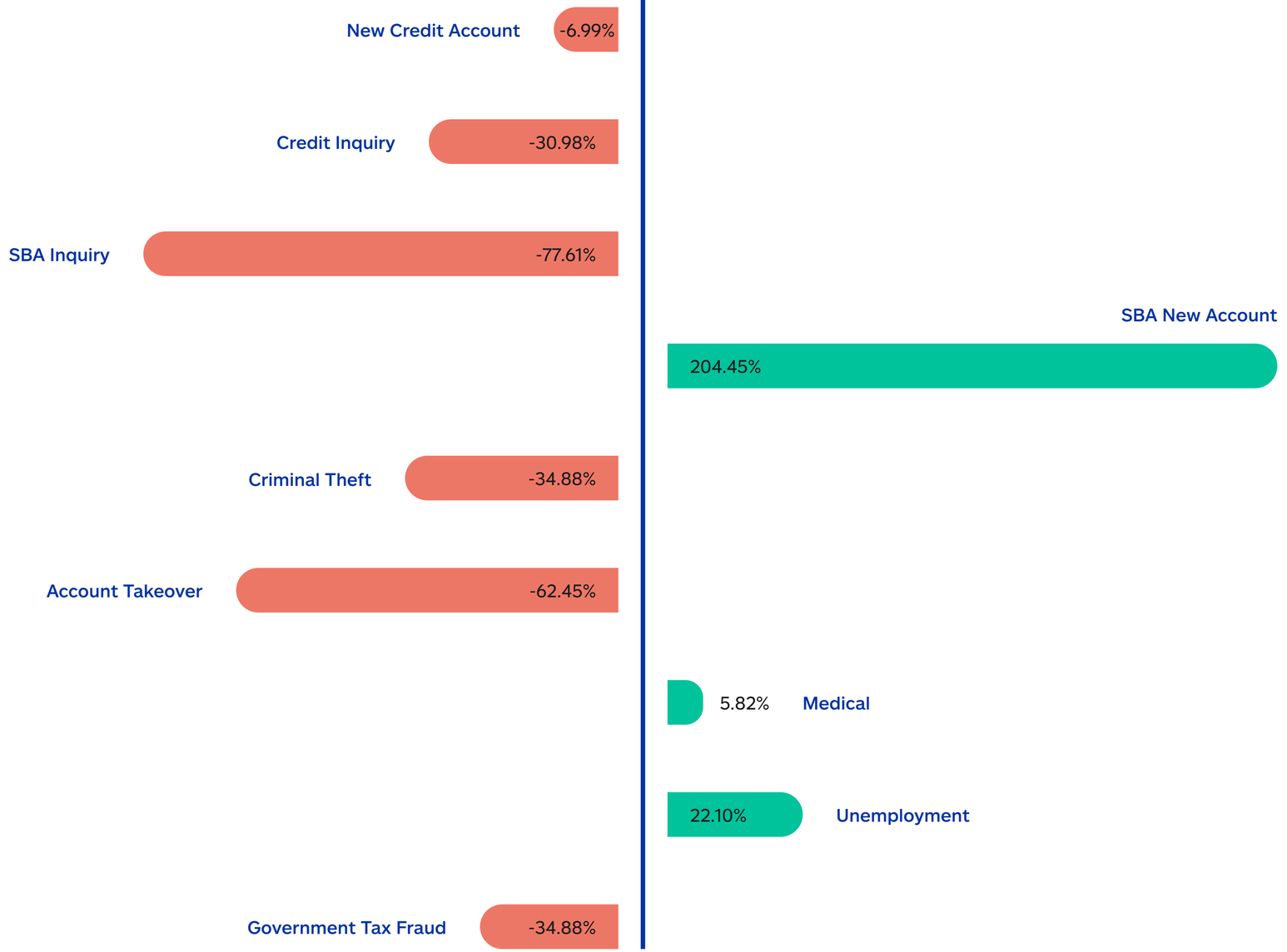
Industries with the most data compromises[1]

- Healthcare
- Manufacturing & Utilities
- Financial Services
- Professional Services

1: Identity Theft Resource Center, "H1 2023 Data Breach Analysis: 2023 Data Compromises Are on a Blistering Pace to Set a New Record"

2: Identity Week, "Breached accounts in Q2 2023: America has highest levels (49.8M), in contrast APAC excluded from fraud table"

Q2 YoY growth



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

ransomware, social engineering, and employee protection

In April, a major chain restaurant conglomerate notified an undisclosed number of employees of a data breach exposing their personal information. This information was stolen in a ransomware attack that shut down 300 restaurants in January.

Hackers don't have to find vulnerabilities in systems architecture to get to sensitive data. According to enterprise cybersecurity provider Sophos, the root causes of ransomware attacks often include compromised credentials (29%), malicious emails (18%), and phishing (13%).[3]

Security-focused industrial sectors like IT, technology, and telecoms report lower rates for exploited vulnerabilities and compromised credentials, but unfortunately have the highest rate (51%) of email-based compromises.[3]

Zero Trust Security policies and robust employee training programs can help minimize the risk to corporate assets while also encouraging teams to stay security-centric with their personal data as well. While enterprise cybersecurity is already a critical focus, digital identity protection can help match the investment in infrastructure with one in workers and their loved ones.

KEY TAKEAWAYS

According to enterprise cybersecurity provider Sophos, the root causes of ransomware attacks often include

29% compromised credentials

18% malicious emails

13% phishing

3: Sophos, "The State of Ransomware 2023"

identity protection and DEI initiatives

October is National Domestic Violence Awareness Month — a time to acknowledge domestic violence survivors and victims. One of the manifestations of domestic violence can include identity theft and fraud as a form of financial abuse. Financial abuse can manifest in different ways — withholding or stealing money, restricting access with an “allowance,” and opening fraudulent accounts using a partner’s identity are just a few.

Allstate Identity Protection is proud to support the efforts of the Allstate Foundation’s relationship abuse program, designed to disrupt the cycle of relationship abuse by providing survivors with education and resources to regain their independence and prevent unhealthy relationships before they start. We’re also rolling out specialized training for our Restoration Specialists on how to recognize signs of relationship abuse and how best to help people who may be experiencing it

about Identity Fraud in Focus

Since 2021, Allstate Identity Protection has provided quarterly Identity Fraud in Focus reports to help consumers, media, and industry experts stay informed about and ahead of the latest digital threats.

“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.”

Allstate SM
IDENTITY PROTECTION