BBB® STUDY: AI tools and Dark Web fuel identity theft, exposing bank accounts and Social Security numbers

BBB

ISSUED: APRIL 2025

INTRODUCTION

STUDY SHOWS HOW SCAMMERS EXPLOIT SECURITY HOLES

Is your financial and personal information being sold on the Dark Web? If you haven't taken the proper precautions, your data may be at higher risk.

It's easy to forget how our personal, everyday data is valuable and sensitive. Passwords, routing numbers, addresses, PINs, security codes on credit cards, dates of birth, Social Security numbers: these are all pieces of information we interact with almost every day. This information helps us keep our calendars, pay bills and do dozens of other vital functions.

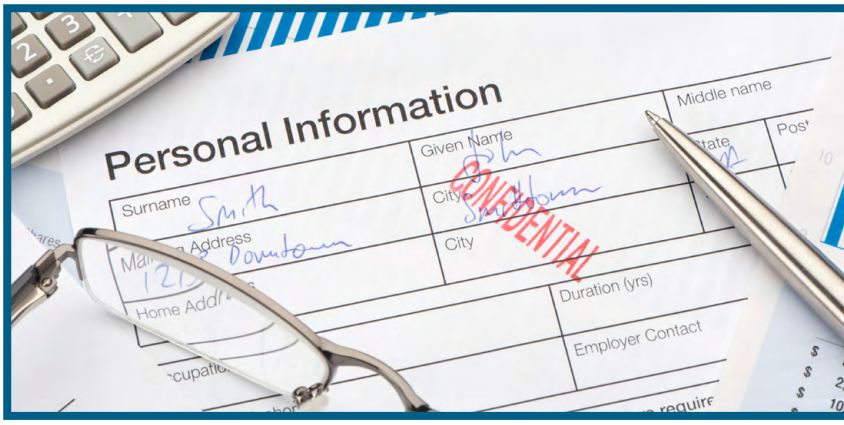
And scammers want to get their hands on all of it.

Over the past three years, Better Business Bureau®, a private, not-for-profit, network of boots-on-the-ground offices which receives no government funding, received over 16,600 reports of high-level identity theft. These incidents involved users realizing some of their most sensitive information was compromised, often only after fraudsters began to use it for their own benefit.

Scammers put this stolen information to use in multiple ways. Sometimes, they sell it for profit online through dozens of Dark Web sites, bundling thousands of stolen identities onto spreadsheets and listing prices like any item for sale online. Other times, consumers are unwittingly roped into scams, with fraudsters taking their name, address, phone numbers and Social Security numbers to open bank accounts, websites and even rent apartments.

As the scammers use the public's information for their ill-gotten gains, wearing their identity like a disguise, scam survivors recall the unsettling effects it has on their lives and livelihoods, creating deep distrust and psychological strain.

To better explain the complex underpinnings of identity fraud, this study examines how scammers exploit holes in personal security, the ways in which scammers use identity fraud to propel other plots and the global scope of the issue.



ABOUT THIS STUDY

This work focuses on patterns of reports from the public about scams they have encountered. Through an analysis of the reports, BBB studies are intended to give consumers, businesses, news media, researchers and regulatory agencies an in-depth understanding of:

- **How these scams work**
- **How to avoid them**
- **What is being done to help curb fraud**

CONTENTS

HOW COMMON IS IDENTITY THEFT?

Identity theft is wide-ranging. It comes in various forms, but the key component is this: Scammers want to take personal information, like a Social Security number, and use it to impersonate the person for illegal gain.

Because identity theft is so widespread and integrated into various scams, someone who is subject to one fraud may not realize their personal information has also been compromised.

"Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance," according to the Federal Trade Commission Identity Theft hub. "In some extreme cases, a thief might even give your name to the police during an arrest."

Many figures related to identity theft deal with instances where someone has their data stolen and used maliciously by a scammer. However, information theft, where someone has their data stolen but is unsure whether it has been used for nefarious purposes, is still an important part of the landscape of identity fraud.

BBB data shows a slight increase in reports since 2021, as well as higher median loss. That information tracks with studies done by credit bureaus, which indicates that the severity of breaches (the type of information being stolen) continues to increase each year.

Robert in Apollo Beach, Florida, told BBB he received a phone call one day about his credit card processing account. The only issue? He never opened an account with the company.

The fraudulently opened account was being used as a payment processor for a fake business the scammer was operating. Given the name of the sham business

by the credit card processing company, Robert learned scammers opened a website with his name in it, used his home address and even procured his social security number and date of birth.

"This is total fraud," Robert said. While the website the scammers opened in Robert's name is down, social media accounts connected to the scam persist. It appears the fraudsters were running a medical supplement scam under his name, pretending to sell multivitamins, among other things.

Zooming out, data from the federal government paints a costly picture. The Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) reported consumers losing over $125 million in 2023, the most recent data compiled by the agency.

Reports to BBB likely represent only a tiny fraction of all cases, according to one study using Federal Trade Commission (FTC) data.

BBB SCAM TRACKER℠ INFORMATION AND IDENTITY FRAUD REPORTS

YEAR	REPORTS	MEDIAN LOSS	SUSCEPTIBILITY
2022	3,972	$408	31%
2023	6,105	$427	38%
2024	6,590	$484	38%

Source: BBB Scam Tracker

HOW COMMON IS IDENTITY THEFT?

Numbers across North America conflict on whether identity fraud has risen within the last few years, with FBI, Federal Trade Commission's Consumer Sentinel Network data and the Canadian Anti-Fraud Centre (CAFC) show a decrease, while credit bureau Transunion showed a 15% increase in 2023, their newest data available.

Every agency and credit bureau, however, warned how identity theft still remains above pre-pandemic levels. FTC data, for example, showed about 650,000 reports of identity fraud to the organization in 2019. The FBI reported about 16,000 cases.

Identity theft is much more than a North American problem. Figures from the European Union show losses of more than $1.1 billion a year from stolen information. "Fraud has changed over the years, with more illicit activities being carried out digitally and often spanning over multiple countries and even continents," said Ville Itala, director-general of the European Anti-Fraud Office in the group's annual report. "What has not changed, is the damage that fraud causes to citizens, markets, institutions and society as a whole."

Identity theft is continuing to evolve internationally, and BBB is warning about a "synthetic" version, where scammers combine pieces of stolen information from several people to create an all-new identity to use for crime and profit.

The staggering amount of identity theft across the globe is due to many aspects, but one of the major factors is the many different forms it takes.

IDENTITY FRAUD REPORTS ACROSS NORTH AMERICA

YEAR	FTC	FBI	CAFC
2021	1,434,477	51,629	31,812
2022	1,107,005	27,922	19,777
2023	1,036,855	19,778	11,375
2024	841,810	TBD	9,487

Source: FBI, IC3, FTC's Consumer Sentinel and the CAFC

WHAT DO SCAMMERS WANT

Nearly every scam contains an aspect of identity theft. Whether it is a stolen password from a brokerage account in an investing scam, a picture of a driver's license in an employment scam or a hacked social media profile in a phishing scam, fraudsters aren't only seeking cash payments, they want data as well.

It may seem as if each individual piece of information is small or insignificant, but the effect on an individual can be massive. And in the aggregate, scammers profit.

Data from the FTC reveals some of the data sources targeted by fraudsters. Stolen information related to bank accounts or credit cards can be costly, while government benefits, a vital resource for many in the United States, could be interrupted in the worst-case scenarios.

But there are also many sub-categories found within BBB Scam Tracker data which reveal areas of risk. Consumers reported stolen social media accounts, hacked dating profiles and high-jacked Facebook groups used to post spam.

In one case, a scammer with their hands on a nursing license number wreaked havoc.

Edelyne in Roosevelt, New York, received a call from someone claiming to be from the FBI in Texas. She told BBB the alleged agent accused her of laundering $3 million.

The man on the phone threatened her livelihood as well, saying her nursing license (for which he had the number) would be suspended if she didn't cooperate. She was directed to share her Social Security number, driver's license, a picture of her car, a picture of herself and her date of birth. Feeling like she had no choice, Edelyne handed over the information.

After that, the man directed her to her bank and told her to wire $10,000 to an account in Hong Kong. Her teller recognized it as a scam and stopped Edelyne from losing her money.

WHAT INFO DO ID THIEVES TARGET?	WHAT DO SCAMMERS DO WITH STOLEN INFO?
SOCIAL SECURITY NUMBER	Open credit cards
NAME	Create utility accounts
ADDRESS	Rack up debts
PHONE NUMBER	Use information in the instance of an arrest
USERNAMES	Take out student loans
PASSWORDS	Apply for government benefits
BANK ACCOUNT NUMBERS	Rent housing
DRIVER'S LICENSE OR IDENTIFICATION CARD	Create investment accounts
TAX INFORMATION	File bankruptcy

WHAT DO SCAMMERS WANT

While it is hard to track down the origin of many scams because so many of them are done by overseas scammers, not all of them are perpetuated by people outside of the country. **Raymond** in Phoenix, Arizona, told BBB he applied for a home loan, only to be rejected. It didn't make sense, as he had kept his accounts in good standing. Raymond was shocked when he pulled his credit report. A man used his Social Security number to rent an apartment, and he owed nearly $10,000 in missed rent. His credit was ruined.

IDENTITY FRAUD TYPE

YEAR	2022	2023	2024*
CREDIT CARD	440,675	416,579	449,032
LOAN OR LEASE	153,598	149,803	176,400
BANK	156,144	136,862	114,608
JOB OR TAX	103,419	89,502	87,470
GOV. DOCS/ BENEFITS	57,783	97,041	70,332
PHONE/ UTILITIES	77,321	79,789	82,626
OTHER	326,521	260,807	358,993
TOTAL	**1,107,004**	**1,036,855**	**1,135,291**

Source: FTC Consumer Sentinel Network

**FTC data allows reports to select more than one category, meaning totals may be higher than the sum of individual categories*

WHAT HAPPENED TO MY STOLEN DATA?

Unfortunately for consumers who have had their information affected in data breaches, their information is far from safe, even if they don't notice any immediate effects.

Scammers unite on surface web, deep web and Dark Web forums to trade information, sell it and give tips on how to continue their ploys. BBB examined more than a dozen active websites to understand how they work, what types of information is being spread and how much scammers can fetch for stolen information.

On a recent post, one fraudster posted a so-called "menu" of information they were offering, with prices attached for the batches of data. On another website, one user claimed to specialize in bank account fraud.

BBB also found several websites devoted to techniques, best practices and lists of stolen information related to "carding," – which is any scam where fraudsters steal credit card or debit information. Tips ranged from how to create secure VPNs, using cryptocurrency to avoid detection when moving money and ways to take advantage of holes in the defenses of common web browsers.

Other websites selling personal information promised big paydays: "CLICK HERE TO MAKE $25,000+/MONTH RIGHT NOW! $3000/DAY PROOF" read one website. Another post on the same site claimed: "WATCH ME EARN $6200 IN 8 DAYS USING UNIQUE METHODS [250+ VOUCHES]"

Even those who know their information is stolen can't always prevent poor outcomes. When **Rossie** in Orlando, Florida, learned some of her information made its way onto the dark web, she was worried about what might happen. Her fears were confirmed when a bank account was opened in her name.

Scammers often use stolen information to open accounts in cases like these. They use those banks to move money around, laundering and making it harder to trace. They might not be open for long, but with enough of them, fraudster operations continue. It can be hard for law enforcement to keep up, as BBB found evidence of posters sharing tips on how to best move money around on hacker forums and let others know when law enforcement is starting to catch on to their methods.

When these hacker forums are taken down, another is often created in its place. For example, the website BreachForums was recently shut down, after building a reputation as one of the most well-known scam websites. One estimate counted its stolen pieces of data at over 14 billion.

WHAT HAPPENED TO MY STOLEN DATA? (CONTINUED)

In the court documents, FBI lawyers presented their case: "Some of the items that are commonly sold on BreachForums include bank account information, social security numbers and other PII (personal identifying information), and account login information for compromised online accounts, such as usernames and passwords to access accounts with service providers and merchants."

"Based on my training and experience, sellers in these marketplaces are typically malicious cyber actors and/or their co-conspirators seeking to monetize data that they obtained through unlawful network intrusions," said the FBI lawyers in the case.

With the growing power of artificial intelligence (AI) tools, scammers can input stolen information in a variety of ways to bolster their tactics.

ExpressVPN, a cybersecurity company, writes about fraudsters using AI tools to search through hundreds of thousands of pieces of information on the dark web to find things like email addresses, leaked credentials and biometric data. They can use the AI to pinpoint specific pieces of "high value" information with a so-called "dark web scan" and then target that person for identity theft.

Not all Dark Web scans are malicious, but when a scammer uses an AI tool built without safeguards, it opens the public to more sophisticated attacks.

"Even if your leaked data doesn't seem important, scammers can piece together multiple leaks over time, creating a full profile that makes you more vulnerable to AI-powered scams," the company says.

Researchers have tested the ability of publicly available chatbots to pull off common scams and found they were easily able to trick people into handing over money. Another study showed AI-powered scams already accounted for $12 billion in losses in 2023. BBB has previously written about how AI tools are helping power scams.

A photo of the website BreachForums after the FBI teamed with other domestic and international sources to take down the website, which was one of the most infamous hacker websites online.

WHAT IS THE BEST WAY TO SECURE YOUR ACCOUNT?

Before a Breach:

- Watch credit reports regularly for unknown accounts
- Use multi-factor authentication whenever possible
- Choose strong and varying passwords across accounts
- Never share personal information unless with a trusted source
- Secure your wi-fi
    - Think about using a VPN (virtual private network)

If you believe your information is compromised:

- Act fast, because scammers may still be actively using your information
- Contact every account holder you believe to be compromised
    - Dispute charges
    - Cancel credit cards
    - Lock accounts
    - Change passwords
- Lock or freeze your credit
- Save documentation as evidence
- File a police report
- Report to BBB, FTC, FBI or CAFC if in Canada
- Avoid credit repair or similar services
- Contact the Identity Theft Resource Center
- Use the BBB ID Theft HQ

What to do in the weeks after the breach:

- Continue to monitor accounts for changed information or further tinkering by scammers who still have access
- Inform friends, family and even your employer so they know how to watch for impostors
- Change passwords on non-hacked accounts if they share a password with a compromised one
    - Consider using a password manager and having unique passwords for each account
- Set up multi-factor authentication
- Monitor your credit reports for unknown accounts and consider a credit freeze
- Be wary of unfamiliar or unprompted mail with personal information

WHAT IS THE BEST WAY TO SECURE YOUR ACCOUNT?

Mona Terry, chief operating officer for the Identity Theft Resource Center (ITRC), told BBB it can be disheartening for people to hear about their information being stolen in data breaches of businesses, because it can feel like there is nothing they can do in those cases.

She urges the public to consider personal data protection as two-fold. Consumers should protect sensitive data whenever possible. But in the inevitable cases of things like data breaches, they should also have monitoring in place on their accounts to catch instances of identity and information theft as soon as possible.

"It is not top of mind for everyone. There is a little bit of fatigue out there. You receive so many notifications," Terry told BBB.

The ITRC sees scams as the most common avenue for identity theft, she said, adding that fraudsters don't just want your money. "They want your money and your information."

The emotional toll of identity theft leaves deep marks because of the intrusion into people's personal lives. 60% of ITRC survivors said they felt like they couldn't trust people anymore. 12% reported feelings or desires of self-harm after instances of identity fraud.

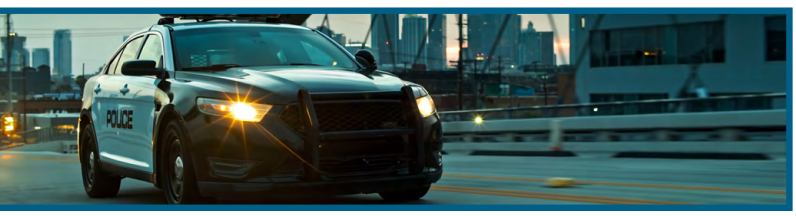
Impostor scams with an identity theft component are rising, Terry said, and tools like artificial intelligence are helping scammers create more convincing fakes. Considering the growing sophistication of fraud, she said scam survivors should not feel guilty about reporting their interactions with scammers.

"This is the scammer's full-time job, and they are good at it," she said.

PROSECUTIONS AND REGULATORY ACTIONS

Law enforcement and regulators are constantly working to take down identity theft hubs, such as BreachForums. But they have also gone after some of the actors behind the sites as well.

Conor Brian Fitzpatrick, 20, of Peekskill, New York, operating under the pseudonym "Pompompurin" on the website, pled guilty in 2023 after the takedown and was sentenced to 20 years of supervised release because of his age and medical circumstances. However, earlier this year, an appeal was filed by the government in the case, alleging he used a virtual private network to access the internet, which was against his court order.



The government appears to be seeking a harsher sentence. Internationally, the FBI, Europol, and United Kingdom's National Crime Agency teamed up in February to take down the 8base ransomware gang, which operated a website used for "dark web data leak and negotiation sites."

Late last year, the European Union attempted to curb identity theft with a new initiative offering a "digital ID" to every citizen in its member nations.

"Member States will be mandated to offer citizens and businesses digital wallets, which can link their national digital identities with proof of other personal attributes like driving licenses, diplomas, and bank accounts," according to the EU regulation.

The digital IDs offer fuller control over sensitive data and prevent unnecessary sharing, a step leaders hope will cut down on identity theft.

RED FLAGS, TIPS & RESOURCES

Red flags of ID Theft:

- Examine domain names closely
- Be wary of emailed links
- Avoid websites with low-quality design
- Texts from unknown sources
- Unexpected voicemails or messages on social media

Tips to avoid ID Theft:

- Regularly check online resources on BBB Scam Studies homepage
- Don't share personal information
- Double check any request for sensitive data like your Social Security number
- Regularly check your credit and review financial statements
- Create strong passwords and change regularly
- Implement multi-factor authentication whenever possible
- Search for reviews and related scams using BBB Scam Tracker
- Use a website checker, like Google's Safe Browsing Tool
- Decide whether to sign-up up for a dark web scanner
- Consider implementing credit freezes or fraud alerts
- Use Annual Credit Report

Where to report ID Theft:

- Better Business Bureau Scam Tracker
- Federal Trade Commission (FTC) or call **877-FTC-Help**
- Federal Bureau of Investigation (FBI) or call **(202) 324-3000**
- Canadian Anti-Fraud Centre - or **1-888-495-8501**
- Find your state's Attorney General online
- Social Security
- Internal Revenue Service

Acknowledgements

This study is a joint project of Better Business Bureaus of Chicago, Dallas, Omaha, San Francisco and St. Louis.

Contributions include data from **BBB Scam Tracker, BBB Institute for Marketplace Trust, IABBB** and various regulatory agencies.

BBB International Investigations Initiative

- BBB Chicago - bbbinfo@chicago.bbb.org
- BBB Dallas - info@nctx.bbb.org
- BBB Omaha - info@bbbinc.org
- BBB San Francisco - info@bbbemail.org
- BBB St. Louis - bbb@stlouisbbb.org

By Brian Edwards, BBB International Investigations Specialist - bedwards@bbbinc.org

Find more information about this study and other BBB scam studies at BBB.org/scamstudies.

BBB's mission is to be the leader in advancing marketplace trust. We do this by:

- Setting standards for marketplace trust
- Encouraging and supporting best practices by engaging with and educating consumers and businesses
- Celebrating marketplace role models
- Calling out and addressing substandard marketplace behavior
- Creating a community of trustworthy businesses and charities

Image Credits: Getty Images

BBB