JUNE 2024

ITRC | IDENTITY THEFT RESOURCE CENTER

2023 TRENDS IN IDENTITY REPORT

idtheftcenter.org • 1-888-400-5530

AIR | ALLIANCE FOR IDENTITY RESILIENCE
ITRC ADVISORY BOARD

*This report was made possible through the support of **ITRC's Alliance for Identity Resilience (AIR) Advisory Board.***

Table of Contents

A Letter from the CEO

In 1964, singer-songwriter (and Nobel prize-winning poet) Bob Dylan sang about the societal changes underway in the United States – "...for the times, they are a-changin'!" Sixty years later, Dylan's lyrics are still true, especially as we learn to take advantage of the benefits and avoid the pitfalls of an increasingly digital world.

Since 2021, the Identity Theft Resource Center (ITRC) has analyzed the trends revealed in the contacts we receive every day from thousands of identity crime victims and individuals seeking information to avoid becoming a victim. The result is this *ITRC Trends in Identity Report* for 2023.

For most of the 25 years the ITRC has been assisting victims, identity crimes were somewhat predictable, even as their volume and velocity increased. Since 2019, though, the rapid changes in society and technology have resulted in wild swings in the scale and types of identity crimes and the number of people impacted by them.

The past 12 months of contacts to the ITRC show some interesting trends:

+ The overall number of victims we assisted declined last year, but...
+ More people reported they had been the victim of multiple identity misuses.
+ More victims reported *attempts* at identity misuse.
+ More people came to the ITRC for help in preventing identity compromises and misuses.

The information gleaned from speaking with victims and curious consumers seeking prevention information – coupled with data from other ITRC and public reports – show an environment where bad actors are more effective, efficient and successful in launching attacks. The result is fewer victims (or at least fewer victim reports), but the impact on individuals and businesses is arguably more damaging.

We focus on three particular conclusions in this report:

- Identity thieves are improving at looking and sounding "legitimate," especially regarding job postings.
- Victims are facing more severe types of identity misuse that can take longer to resolve.
- Identity thieves already have enough information to impersonate individuals (and businesses) to open new financial and other types of accounts.

At first glance, the information from victims published here, along with data from other research reports, can be contradictory and even a little confusing. *"How can data breaches be up, but the number of victims down?" "How can there be fewer reports of identity misuse, but the impacts so much greater that 16 percent (16%) of victims contemplated suicide?"*

The answers to these and other questions surrounding identity crimes are becoming clearer as more reinforcing data like this *Trends in Identity Report* is released. However, one conclusion requires no additional information: ***There are still too many identity crime victims and too few resources to help them.***

Supporting victims is the core of our mission – providing the assistance identity crime victims need to regain control of their stolen and compromised personal information and help them repair the damage done to their identities and lives.

As you read this report, I encourage you to think about where you, your friends and your family would turn if an identity criminal took advantage of someone in that circle. How would your employer or you as a business leader react if your organization was the victim of business identity theft? In both instances, what can you do today to help prevent your identity from being misused or compromised, and where would you go to learn how to do it?

For 25 years, the answer has been, and remains, the Identity Theft Resource Center.

Eva Velasquez,
PRESIDENT & CEO

Eva C. Velasquez

Identity Theft Resource Center
June 2024

Key Takeaways and Trends

2023 Takeaways

The number of victims assisted by ITRC Victim Advisors declined in 2023.

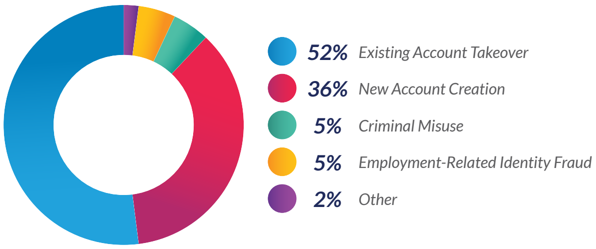
ITRC Victim Advisors assisted 10,904 new victims of identity misuse, attempted misuse or identity compromise. That's down 16 percent (16%) from the previous year.

The new victims reported 13,197 instances of identity crimes, an 11 percent (11%) drop from 2022.

The percentage of new victims who reported multiple instances of identity crimes grew last year.

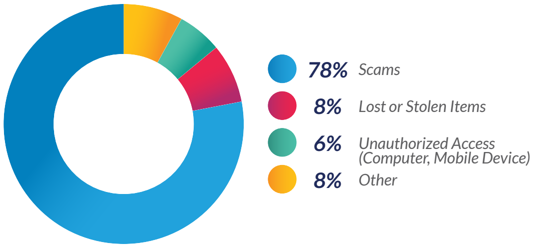
Existing Account Takeover (52%) and New Account Creation (36%) were the most reported forms of identity misuse, followed by crimes committed using compromised personal information (5%) and employment-related identity fraud (5%).

Figure 1 | *Top-Reported Forms of Identity Misuse*



Scams (78%), Lost or Stolen Items (8%) and Unauthorized Access to a computer or mobile device (6%) were the most reported forms of identity compromise.

Figure 2 | *Top-Reported Forms of Identity Compromise*



Reports of attempted identity misuse reports increased by 11 percent (11%), most often related to a financial account.

The number of people seeking prevention or protection information from the ITRC nearly doubled compared to the previous year.

Victimization Trends

TREND 1
Identity thieves are improving at looking and sounding "legitimate," especially regarding job postings. It's likely generative AI-related.

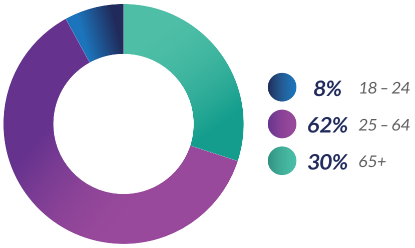
TREND 2
Victims are facing more severe types of identity misuse.

TREND 3
Identity thieves already have enough information to open new lines of credit and other types of accounts.

2023 Demographics

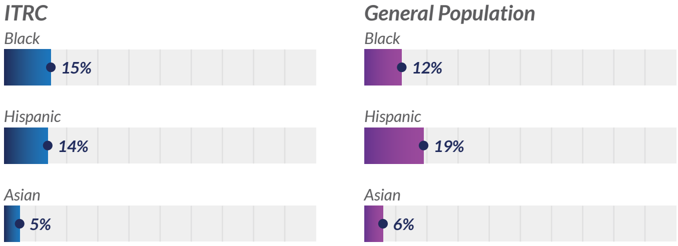
The vast majority of victims – 62 percent (62%) – fell within the age range of 25 to 64 years old. Victims 65+ years old only accounted for 30 percent (30%).

Figure 3 | *Age*



Members of Black communities contacted the ITRC for victim assistance at a higher rate compared to the general population (15% vs. 12%). Hispanic (14% vs. 19%) and Asian (5% vs. 6%) community members were under-represented in the number of victims contacting the Center.

Figure 4 | *Ethnic Communities Contacting ITRC vs General Population*



Victims rated ITRC Victim Advisors 4.9 out of 5 for service satisfaction, dedication to assisting victims and knowledge in post-support surveys.

Victims from all 50 states connected with the ITRC during the year. However, victims who lived in California, Florida, Texas, New York and Pennsylvania contacted the ITRC more often.

The *Trends in Identity Report* looks at the trends in identity based on information from the victims that contact the ITRC. For the report, the ITRC examined the wide range of identity crimes committed against people as reported by the victims of those crimes.

ITRC IDENTITY THEFT RESOURCE CENTER

AIR ALLIANCE FOR IDENTITY RESILIENCE ITRC ADVISORY BOARD

This report was made possible through the support of ITRC's Alliance for Identity Resilience (AIR) Advisory Board.

2023 Reported Identity Crimes

13,197 TOTAL CRIMES REPORTED

New Cases Reported
11% Decrease
FROM 2022

ATTEMPTED MISUSE
1% OF ALL VICTIMS

ACTUAL MISUSE
38% OF ALL VICTIMS

IDENTITY COMPROMISE
53% OF ALL VICTIMS

REQUESTING PREVENTION
7% OF ALL VICTIMS

2023 Identity Compromises

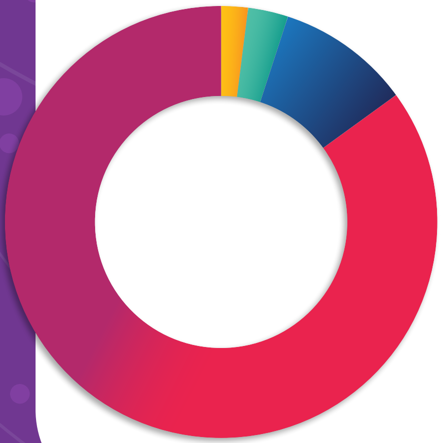
78% COMPROMISES DUE TO A SCAM

2% Decrease
FROM 2022

JOB SCAMS ON THE RISE
118% INCREASE IN 2023

GOOGLE VOICE REMAINS TOP SCAM
60% OF ALL SCAMS IN 2023

Number of Crimes Reported Per Victim in 2023



●	**86%**	*One Incident*
●	**10%**	*Two Incidences*
●	**3%**	*Three Incidences*
●	**2%**	*Four or More Incidences*

2023 Identity Misuse

52% EXISTING ACCOUNT TAKEOVER (ATO)

35% NEW ACCOUNT CREATION

FINANCIAL
53% OF ALL MISUSED ACCOUNTS

NON-FINANCIAL, NON-GOVERNMENT
35% OF ALL MISUSED ACCOUNTS

FEDERAL
6% OF ALL MISUSED ACCOUNTS

STATE
6% OF ALL MISUSED ACCOUNTS

Glossary of Terms

For purposes of this report the ITRC uses standard industry terms as defined by the National Institute of Standards & Technology (NIST) as well as specific definitions develop by the ITRC.

Account Takeover (ATO) – When an unauthorized person gains control of an existing account. ATO includes financial accounts such as bank accounts or non-financial accounts such as social media accounts.

Cases – Instances of identity compromise or misuse reported by people who contact the ITRC Contact Center.

Contacts – Individuals who contacted the ITRC Contact Center for any reason, including prevention as well as instances of identity compromise and misuse.

Data Breach – A data event where personal information is removed by malicious action or by an error from a database or system where it was created, collected, processed, or maintained.

Data Exposure – An event where personal information is available for viewing or download but NOT copied or removed from the database or system where it was created, collected, processed, or maintained.

Identity Compromise – When a person's personally identifiable information (PII) has been exposed in a data breach, a cybersecurity failure, or because of a scam.

Identity Crimes – The use of stolen personally identifiable information (PII) to commit a crime.

Identity Fraud – The use of stolen personally identifiable information (PII) to commit fraud.

Identity Misuse – The use of someone's stolen personally identifiable information (PII) to commit an identity crime.

Identity Theft – The act of stealing someone's personal information.

New Account Fraud – Opening new credit card or bank accounts using stolen PII.

Personally Identifiable Information (PII) – Personal information such as name, date of birth, driver's license number, Social Security number, etc. The definition of PII varies by state, but often includes logins and passwords.

Social Engineering Techniques – Using personal interactions and emotional manipulation to entice someone to willingly give a criminal their personally identifiable information (PII).

Overall Victim Services

- + *Year-Over-Year Comparison*
- + *Victim Assistance Satisfaction Ratings*

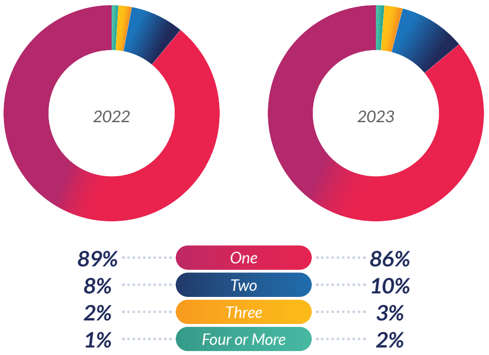
Overall Victim Services

In the 12 months from January 1 through December 31, the Identity Theft Resource Center (ITRC) assisted 10,904 "new" victims of identity theft who were impacted by 13,197 instances of an identity crime.

The overall number of victims assisted declined 16 percent (16%) compared to the previous 12 months, while new cases of identity crimes reported to the ITRC were down 11 percent (11%) year-over-year.

Eighty-six percent (86%) of victims reported being victims of a single identity crime during the period during which a higher percentage of victims experienced multiple instances of identity crimes compared to the previous year.

Figure 5 | *Number of Identity Crime Instances*



The primary channel of choice for contacting the ITRC about an identity theft concern was by phone (71% of victims), followed by chat (26%), email (2%) and the ITRC's website form (1%).

Figure 6 | *Method Used to Contact ITRC*

	2022	2023
Phone	65%	71%
Chat	33%	26%
Email	2%	2%
Web Form	<1%	1%
Letter	<1%	<1%
Social Media	<1%	<1%

More victims chose to reach out via phone vs. chat compared to the previous reporting period.

For the past two years, victims primarily contacted the ITRC about compromised personal information (53%) and information misuse (38%). In 2023, we saw a slight increase in the number of victims of attempted misuse.

Figure 7 | *Reason Why Victims Contacted ITRC*

	2022	2023
Attempted Misuse	1%	2%
Actual Misuse	40%	38%
Compromise	55%	53%

Of the victims who provided their state of residence, victims in the following states contacted the ITRC most frequently about their identity theft concerns – California, Florida, Texas, New York and Pennsylvania.

Figure 8 | *Top Ten States by Contacts*

	2022		2023
California	12%	California	11%
Texas	7%	Florida	5%
Florida	6%	Texas	5%
New York	6%	New York	4%
Pennsylvania	3%	Pennsylvania	2%
Illinois	3%	Illinois	2%
Georgia	3%	Ohio	2%
North Carolina	3%	Georgia	2%
Ohio	3%	North Carolina	2%
Michigan	2%	New Jersey	2%

Victim Assistance Satisfaction Ratings

Victims rated the ITRC's Victim Advisors 4.9 out of 5 for satisfaction with the service provided, advisor dedication to assisting the victim and advisor knowledge.

The ratings are based on victim surveys compiled by an independent service, *Get Feedback*.

> *[Advisor] was amazing! Calmed my worst concerns, gave excellent actionable advice and was truly a great person!*

> *Everything [the advisor] said was understandable, and I learned more about it that I didn't think possible. Thanks, everyone, for your amazing, caring attitudes. I really felt like you cared.*

> *[Advisor] was very knowledgeable, polite and clear. Having your identity stolen is a very difficult thing to handle, and it helps to have guidance as the steps to prevent further harm are not easy or clear.*

> *[Advisor] was seriously awesome. Having your identity messed with makes you feel so vulnerable to an invisible bad guy, and she gave me a list of tangible things I can do today to protect myself and bring back the feeling of safety.*

> *[Advisor] was absolutely incredibly dedicated to assisting me and addressing all concerns. I received more solid advice from her in 5 minutes than 8 hours of googling, etc. They know their stuff!*

Victimizations

- + Attempted Misuse
- + Actual Misuse
  - Summary
  - By Account Category
  - By Account Type
- + Identity Compromise

Identity Crime Type – Attempted Misuse

The ITRC reports victim contacts into three major categories:

***Attempted Misuse** - When a bad actor attempts to use another individual's personal information*

***Actual Misuse** - When a bad actor misuses another individual's personal information*

***Identity Compromise** - When an individual's personal information is exposed or stolen in a data breach, by a system or human error, or a physical attack*

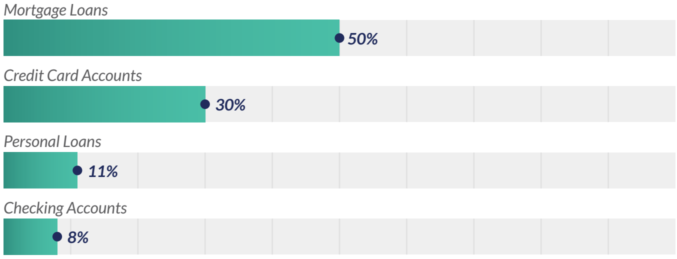
Attempted misuse affected one percent (1%) of all identity crime victims in 2023.

There was an 11 percent (11%) increase in reports of attempted misuse from 2022 to 2023.

The primary increase in reports of attempted misuse was with financial accounts. There was an overall decrease in reports of attempted misuse of government and non-government, non-financial accounts.

There was an increase in reports of attempted misuse with checking accounts year-over-year (8%), credit card accounts (30%), mortgage loans (50%) and personal loans (11%).

Figure 9 | *Increases in Attempted Misuse*



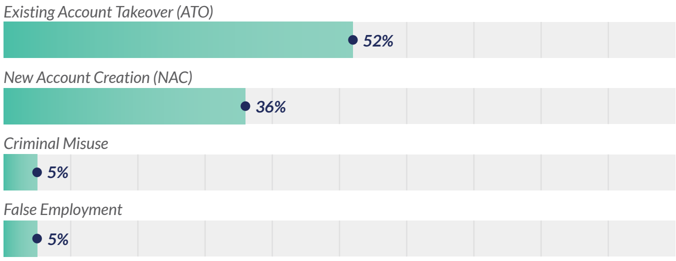
Identity Crime Type – Actual Misuse

Actual Misuse Summary

Actual misuse affected 38 percent (38%) of all identity crime victims in 2023.

The most reported types of misuse were Existing Account Takeover (ATO) (52%) and New Account Creation (NAC) (36%), followed by crimes committed using compromised personally identifiable information (PII) (5%) and False Employment (5%).

Figure 10 | *Top Reported Types of Misuse*



There was a 117 percent (117%) increase in the number of reports of False Employment year-over-year.

> **VICTIM STATEMENT**
> *I get SSI benefits, and I received a letter saying that I made $99,337 in 2022, and that is impossible cause I been disabled since 2021, and I have all my doctors that will tell you, I get retirement benefits so SSI is taking $1,000 a day to pay for overpayments.*

There was a 23 percent (23%) increase in reports of criminal misuse of PII compared to the previous report.

> **ADVISOR NOTES**
> *Caller reached out on behalf of her son, who is in a mental hospital and has been a victim of criminal I.D. theft. Caller states they were notified by a letter from an attorney regarding the jail booking. The ID theft took place in Missouri. Caller and victim are in Montana.*

> **VICTIM STATEMENT**
> *My sister has stolen my identity, and now I have warrants in several different counties. I can prove without reasonable doubt that she did this, but I can't afford to keep missing work for all these court dates. I am gonna lose my job... I have two court dates in a week for something that I didn't do.*

There was a nine-percentage point decrease in reports of Existing ATO during the 12-month reporting period. There was a four-percentage point increase in reports of NAC.

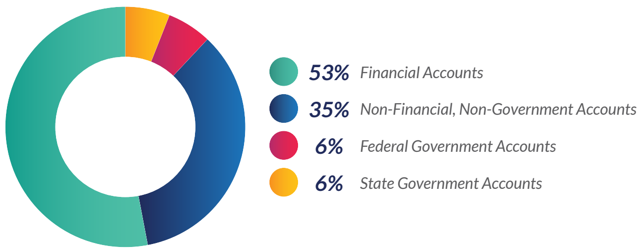
Actual Misuse by Account Category

Actual Misuse falls into two primary categories – Existing ATO and NAC – involving one or more types of accounts.

ATO involves a criminal gaining account access using stolen credentials, malware or after a victim shares personal information with a person they believe to be trustworthy. NAC is the result of a criminal applying for or creating a new account using stolen or coerced personal information.

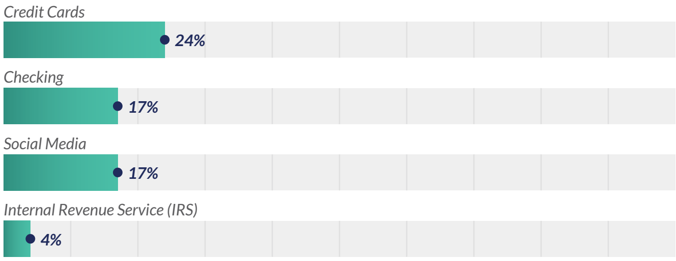
In the 12-month reporting period, the type of accounts most often reported as being misused fell into four categories: Financial accounts (53%), followed by Non-Financial, Non-Government Accounts (35%), Federal Government Accounts (6%) and State Government Accounts (6%).

Figure 11 | *Actual Misuse by Account Category*



Within the four categories, the top account types that were impacted by criminal misuse were credit cards (24%), checking (17%), social media (17%) and Internal Revenue Service (IRS) (4%).

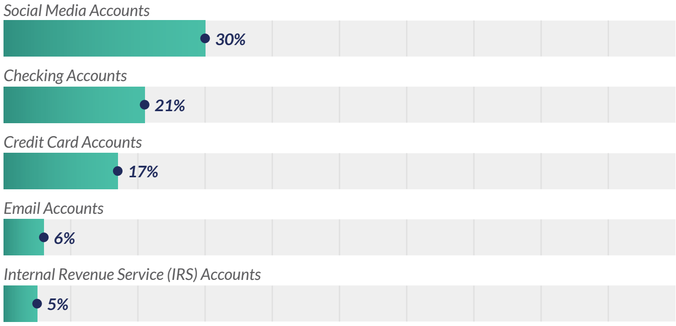
Figure 12 | *Top Account Types of Misuse*



Existing Account Takeover (ATO) – 52 Percent (52%) of All Misuse Cases

In 2023, Existing ATO primarily impacted social media accounts (30%), checking accounts (21%), credit card accounts (17%), email accounts (6%) and IRS accounts (5%).

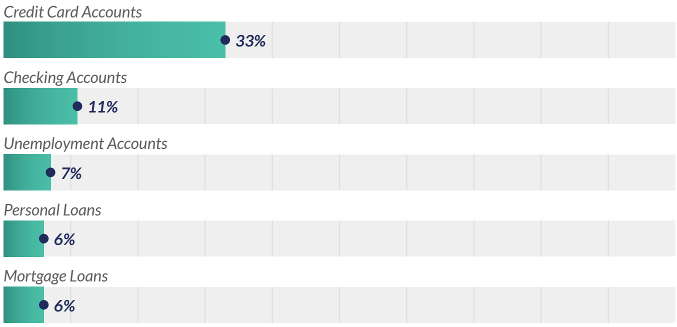
Figure 13 | *Top ATO Account Types*



New Account Creation (NAC) – 35 Percent (35%) of All Misuse Cases

NAC primarily occurred with credit card accounts (33%), checking accounts (11%), unemployment accounts (7%), and personal (6%) and mortgage (6%) loans.

Figure 14 | *Top NAC Account Types*

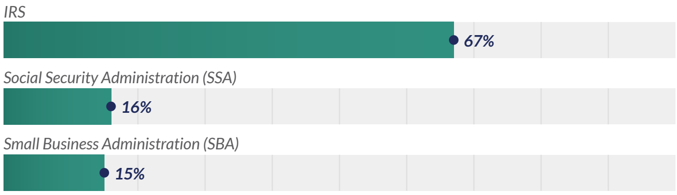


Actual Misuse by Account Type

Federal Accounts – Six Percent (6%) of All Misused Accounts

The top Federal Government accounts impacted by identity crimes were the IRS at 67 percent (67%), Social Security Administration (SSA) at 16 percent (16%) and Small Business Administration (SBA) at 15 percent (15%) of federal accounts.

Figure 15 | *Top Misused Federal Government Accounts*



Seventy-seven percent (77%) of IRS accounts reported as misused were primarily impacted by ATO.

ADVISOR NOTES

Victim states that she believes she is a victim of I.D. theft because when her son tried to claim her on his taxes, it was getting rejected, saying she had already filed. She states she has been living with her son for almost two years and did not file or give anyone permission to do so.

ADVISOR NOTES

Victim stated that years ago their accountant's system was breached and taxes were filed in her name, as well as her husband and her 12-year-old son.

SBA accounts - 15 percent (15%) of all government accounts compromised - were only impacted by NAC attacks.

Reports of new SBA accounts increased by 83 percent (83%) in the past year.

ADVISOR NOTES

Victim reached out and said that an SBA loan was opened under his name two years ago. The victim found out about this three weeks ago when he got a letter in the mail regarding the matter. The victim says that this account is now in collections.

Most SSA accounts (80%) were primarily impacted by ATO compared to 20 percent (20%) affected by NAC.

VICTIM STATEMENT

My grandmother has been in the hospital since February 10 until March 4, where she had passed. In that time, her food stamps and her SSI has been used. Her son and grandson had ahold of her belongings.

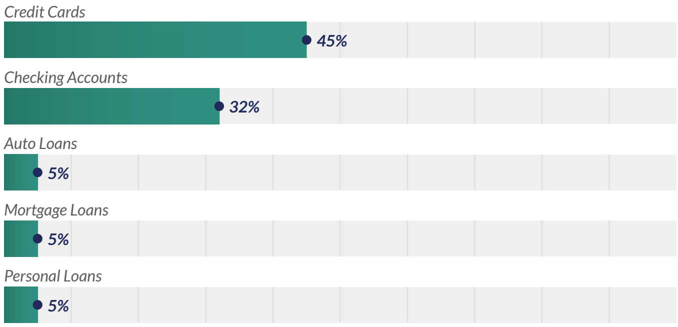
ADVISOR NOTES

Victim states she got a letter from SSA. She read the letter to me, and it was to let her know they had received her request to change her authorized payee. She lives in a nursing home and has not done this.

Financial Accounts – 53 Percent (53%) of All Misused Accounts

The top financial accounts impacted by identity crimes were credit cards (45%), checking (32), auto loans (5%), mortgage loans (5%) and personal loans (5%).

Figure 16 | *Top Misused Financial Accounts*



Credit cards impacted by identity crimes were primarily impacted by NAC (59% of credit card accounts) vs. ATO (41% of credit card accounts).

There was a seven percent (7%) increase in reports of fraudulent new credit cards in 2023.

VICTIM STATEMENT

I have recently become a victim of identity theft, I had a fraudulent credit card opened in my name and had charges done on the card for the span of a year without my knowledge, upon discovery of the fraudulent account, I have done most of the necessary steps that would normally be required of me...however the bank has not been very cooperative... I have had my fraud claim denied twice already... I am worried that they may deny the fraud claim for a third time, if this happens, I am not sure what to do. Legal action may end up costing me more than the fraudulent charges in question...

Checking accounts impacted by identity crimes were primarily impacted by ATO (71% of checking accounts) vs. NAC (29% of checking accounts).

ADVISOR NOTES

Victim says her credit union account was taken over. She was notified via email that her funds were gone. She was $30,000 overdrawn. They provided her with the names of the banks where the funds were sent. Her bank is refusing to open an investigation or request the funds back.

ADVISOR NOTES

Victim stated she got a message from her bank asking that she confirm a transaction, followed by a phone call from a number she had spoken to her bank from before. She provided the same information she had in the past when locking her account or disputing the fraudulent charge. Then she realized they had taken $50,000 out of her account, transferred it to three separate accounts created with her name, and ultimately transferred it via Zelle.

Ninety-seven percent (97%) of auto loans, 87 percent (87%) of mortgage loans and 99 percent (99%) of personal loans were impacted by NAC vs. existing ATO.

There was a 20 percent (20%) increase in fraudulent new auto loans in 2023 vs. 2022, a 30 percent (30%) increase in fraudulent new mortgage loans in 2023 vs. 2022 and an 18 percent (18%) increase in fraudulent new personal loans in 2023 vs. 2022.

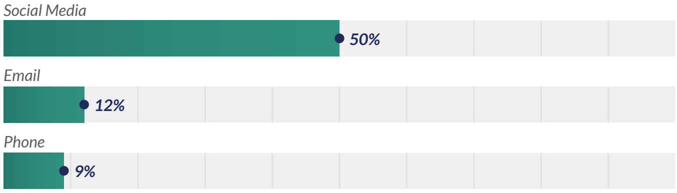
VICTIM STATEMENT

My name is being used in several different ways. I received a credit report in hopes to rent an apartment and was denied due to a very poor score, which is caused a lot by an auto loan and a home loan, both unpaid or unkept, in Washington state under my name. I have never lived in Washington, much less pulled out any kind of major loan or loans. I actually have had quite the struggle with my hopes for my future because of the amount of debt caused from this and many other instances involving my name that I have not authorized.

Non-Financial, Non-Government Accounts – 35 Percent (35%) of All Misused Accounts

The top non-financial, non-government accounts impacted by identity crimes were social media (50%), email (12%) and phone (9%).

Figure 17 | *Top Misused Non-Financial, Non-Government Accounts*



There was a 55 percent (55%) decrease in the number of social media accounts reported as taken over in the past 12 months.

ATO (98%) was still the primary type of identity crime involving social media accounts vs. NAC.

VICTIM STATEMENT

My Facebook account was hacked in May of this year. I tried everything to recover it and tried reaching out to Facebook in any type of way. I had my family and friends report the account but nothing has happened. The hacker is reaching out to my family and friends. I would hate for them to fall victim of a scam. All I want is to either recover the account or have it permanently deleted so the hacker can't impersonate me. Knowing that this hacker is using my profile to reach out to my family and friends is causing me to have anxiety.

Email accounts were primarily impacted by ATO (97%).

ADVISOR NOTES

The victim advised that all his emails and accounts were compromised in a data breach. He stated he saw another browser on his website, and it stated that new unknown devices opened it. Because his Google account was accessed, he states that all accounts, including Disney+ and Facebook, were compromised because they had access to his emails.

Mobile phones were primarily impacted by NAC (61%). There was a 48 percent (48%) increase in reports of new phone accounts using a victim's information last year compared to the previous year.

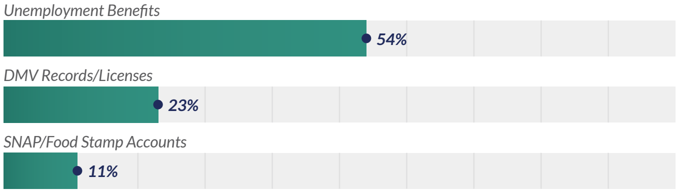
ADVISOR NOTES
The victim advised that someone opened a [cell phone] account in her name. The bill came to her new address in the amount of $1200.00 on 1/25/2023 and was already in a past-due status. The victim contacted [cell phone company] and discovered the account was already closed.

ADVISOR NOTES
Victim called stating someone in Colorado has stolen his identity and charged several thousand dollars on an account with [cell phone provider] in 2022. He called [cell phone provider] and was told that the debt had been sent to a collections company, but he has not called them yet. He does not know how someone got his information; his bank told him about it because he inquired about his credit score dropping.

State Accounts – Six Percent (6%) of All Misused Accounts

Identity crimes involving State Accounts primarily impacted unemployment benefits (54%), DMV records/licenses (23%) and SNAP/food stamp accounts (11%).

Figure 18 | *Top Misused State Account Types*



The number of significant decreases in reports of identity-related unemployment benefit fraud, but the number of individual victims still remains well above pre-pandemic levels. Unemployment accounts were primarily impacted by NAC (88%) vs. ATO (12%).

There was a 71 percent (71%) decrease in existing unemployment accounts being compromised in 2023 vs. 2022. New unemployment accounts declined 35 percent (35%) compared to the previous.

Compromised DMV accounts were more likely to be reported as ATO compared to NAC: 63 percent (63%) vs. 37 percent (37%).

ADVISOR NOTES
Victim states she received an email on 7/3/2023 stating that the duplicate NM license she ordered was sent to a specific address. She had not applied for a duplicate license, and the address was not hers.

ADVISOR NOTES
Victim states she received an envelope in the mail containing a copy of her I.D. The person sent it to her, thinking she had lost it, but she realized her I.D. was with her and she had not lost it. She states it is a pretty good copy, and all the info is the same as her I.D.

More new SNAP accounts were created than compromised – 59 percent (59%) vs. 41 percent (41%).

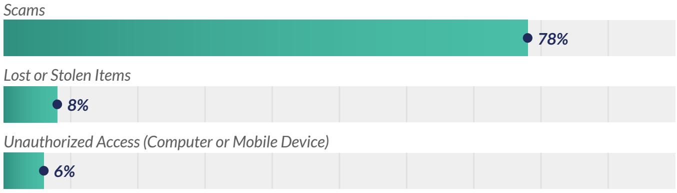
ADVISOR NOTES
Caller reached out on behalf of his uncle, who has had his SSN misused. He said an old group of his caretakers have stolen his uncle's I.D. and are receiving EBT benefits.

Identity Crime Type – Identity Compromise

An identity is compromised when a person's PII has been exposed, but there's no evidence that the information has been misused. PII is frequently compromised in a data breach, but its personal information can also be exposed in a cybersecurity failure or self-compromised as part of a scam.

Among victims who contacted the ITRC in the 12-month reporting period, the primary cause of personal information compromise was Scams (78%), Lost or Stolen Items (8%) and Unauthorized Access to a computer or mobile device (6%).

Figure 19 | *Top Causes of PII Compromise*



Scams – 78 Percent (78%) of All Identity Compromise Victims

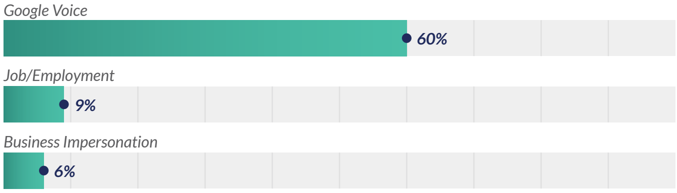
Overall reports of scams to the ITRC decreased 18 percent (18%) from the prior year.

The most common non-sensitive PII shared with scammers was a phone number (36%), a name (27%) and an address (9%).

The most common sensitive PII shared with scammers were full or partial Social Security numbers (SSNs) (6.5%), date of birth (6.3%) and driver's license numbers (5.7%).

The top scams reported in 2023 were Google Voice (60%), job/employment (9%) and business impersonation (6%).

Figure 20 | *Top Scams in 2023*



Reports of the Google Voice scam decreased 16 percent (16%) from the prior year. Google Voice scams were primarily carried out through Facebook and other social media platforms.

Reports of job/employment scams increased 118 percent (118%) in 2023. Job/employment scams were primarily carried out through websites, typically LinkedIn or job search platforms.

ADVISOR NOTES

Victim reached out and said that he had fallen victim to a job scam. The victim said that he was attempting to apply for a job online. He said he spoke to people he didn't feel comfortable with, so he decided to look them up and found out that they used other people's images. The victim said he gave them his SSN, Driver's License picture, and address.

ADVISOR NOTES

I had a potential employer get me in for a virtual interview, and I gave them my name, address and a photo of my I.D. Once the interview was over, I did some digging, and it looks like the company is a scam.

Reports of business impersonation scams decreased 19 percent (19%) from 2022 to 2023. Business impersonation scams were primarily carried out by phone – either through the scammer contacting the victim or the victim searching for a phone number via a website search engine and unknowingly finding the wrong phone number.

> **ADVISOR NOTES**
>
> *Victim reached out and said that she fell for a scam. She was looking for YouTube TV customer service and Googled for a number. She called the first number she saw, which turned out to be a scammer. She lost $5,500 during this process. The victim said she tried to dispute this with her bank, but they denied the dispute.*

> **ADVISOR NOTES**
>
> *The victim received a phone call from someone claiming to be from Amazon, and they said that orders were placed under her name and they were verifying if she ordered them. She told them she doesn't have an Amazon account. They told her they were going to transfer her to the Social Security Administration in Atlanta. They then told her they were going to seize her accounts because money was being transferred. They asked how much money she had in her bank accounts, and she told him. She did provide a photo of her driver's license.*

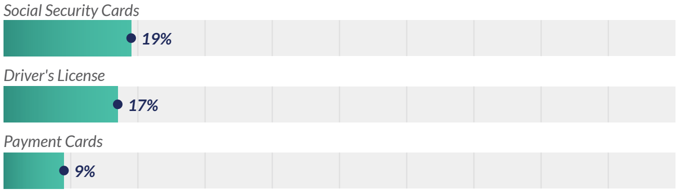
Lost or Stolen Items – Eight Percent (8%) of All Identity Compromise Victims

The number of victim contacts linked to Lost or Stolen Items decreased 66 percent (66%) year-over-year.

There were more reports of stolen documents (86%) than lost documents.

The most common documents reported as stolen were Social Security cards (19%), followed by a driver's license (17%) and payment cards (9%).

Figure 21 | *Most Common Documents Reported Stolen*



Preventative Information and Education

- + *Risk Prevention Through ITRC*
- + *Victim Demographics*
- + *Third-Party Reports*
- + *Identity Criminal Profile*

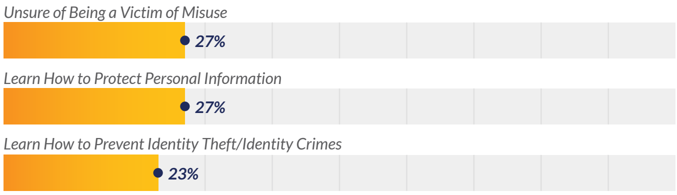
Risk Prevention Through ITRC

The number of people who contacted the ITRC's contact center in the 12-month reporting period seeking information on how to reduce the risk of becoming an identity crime victim or protect their personal information (7%) nearly doubled over last year (3%).

Victims who requested preventative information primarily contacted the ITRC because they had been contacted by an identity criminal but had not shared any information and wanted to know what to do (47%).

Nearly one-third (31%) of victims wanted additional information because they were unsure if they were a victim of misuse (27%) and wanted to learn how to check. A similar number (27%) wanted to learn how to protect their personal information, and 23 percent (23%) wanted to know how to prevent identity theft or other identity crimes.

Figure 22 | *Victims Seeking Additional Information*



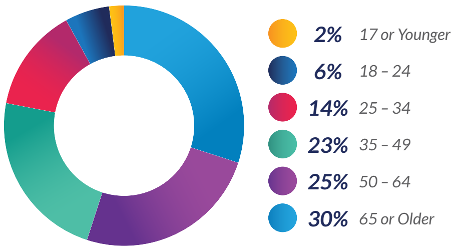
Victim Demographics

The ITRC collects demographic information (age, household income, ethnicity and gender) from victims who are willing to provide the information on an optional basis. The data is used for federal grant reporting and to help the ITRC understand which groups, if any, may be targeted for various identity crimes and to identify which groups may benefit from additional education and outreach about identity crimes.

Age

Despite the popular belief that older consumers (65+ years) are more susceptible to identity crimes, self-reported age information reinforces other ITRC research, the findings of other organizations, and government agencies that younger consumers fall victim to identity crimes more frequently. Of the victims who were willing to share their age range, the vast majority (62%) fall within a range from 25 to 64 years of age. The single largest category includes victims who are 65 or older.

Figure 23 | *Age*



Types of Misuse Based on Age:

Victims aged 35 – 49 (30%) reported more instances than any other age category.

Checking accounts (28%) and credit card accounts (21%) were the most compromised by ATO accounts. The highest number of ATO reports were from victims aged 65 or older (27%).

Victim PII was used in NAC to open credit card accounts (37%), checking accounts (9%) and mortgage loans (8%). The highest number of new account fraud reports were from victims in the 35 – 49 age range (27%).

Types of Compromise Based on Age:

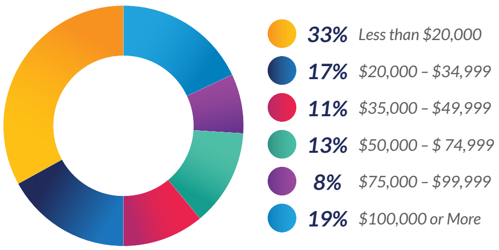
Victims aged 65 or older reported the highest number of identity compromises through breaches and scams.

Victims aged 35 – 49 reported the highest number of identity compromises through physical items being lost or stolen and through unauthorized access to a computer or mobile device.

Income

Victims aged 35-49 reported the highest number of identity compromises through physical items being lost or stolen and through unauthorized access to a computer or mobile device.

Figure 24 | *Income*



Types of Misuse Based on Income:

Checking accounts (31%) and credit card accounts (19%) were most often compromised by ATO attacks. The highest number of ATO reports were from victims whose household income was less than $20,000 (36%).

Victim PII was used most often in NAC attacks to open credit card accounts (38%), checking accounts (9%) and mortgage loans (9%). The highest number of new credit card account reports were from victims whose household income was more than $100,000 (35%).

Types of Compromise Based on Income:

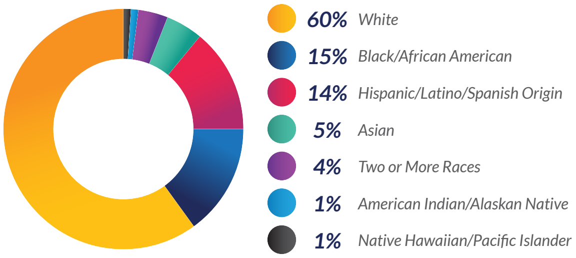
Victims whose household income was over $100,000 (22%) reported the highest number of identity compromises through scams, followed by victims whose household income was less than $20,000 (20%) and victims whose household income was $50,000 to $74,999 (19%).

Victims whose household income was less than $20,000 comprised more than half (53%) of identity compromises through unauthorized access to a computer or mobile device.

Ethnicity

Of the victims who were willing to share their ethnicity, we received the highest number of reports of identity crimes from victims who self-identified as White (60%), followed by Black or African American (15%) and Hispanic or Latino, or Spanish Origin of any race (14%).

Figure 25 | *Ethnicity*



Types of Misuse Based on Ethnicity:

The highest number of new account fraud reports were credit card accounts (36%). Victims who self-identified as White (60%) reported the highest instance of new credit accounts being opened, followed by Hispanic or Latino, or Spanish Origin of any race (18%).

Types of Compromise Based on Ethnicity:

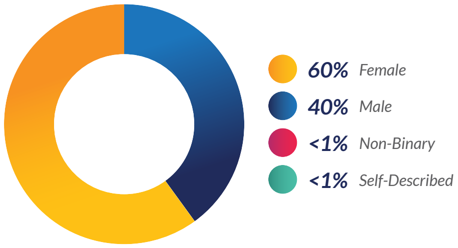
Victims who self-identified as White (42%) reported the highest instance of physical items being lost or stolen, followed by Hispanic or Latino, or Spanish Origin of any race (22%) and Black or African American (21%).

Personal information compromised due to a data breach made up only six percent (6%) of self-reported types of compromise, with the data breaches being primarily reported by victims who self-identified as White (70%) and Asian (13%).

Gender

Of the victims who were willing to share their gender, we received the highest number of reports of identity crimes from victims who self-identified as Female (60%) followed by Male (40%).

Figure 26 | *Gender*



Types of Misuse Based on Gender:

Female victims (94%) reported far more instances of New Medical Insurance Account creation than victims who identified as Male (6%); however, these instances of identity misuse accounted for only three percent (3%) of NAC.

Types of Compromise Based on Gender:

Significantly more victims who identified as Female (78%) than Male (22%) reported being victims of Unauthorized Access to a computer/mobile device.

Third-Party Reports

Victims of identity crimes primarily reported identity crimes that happened to themselves (92%). A small number of victims also reported identity crimes on behalf of a Spouse/Partner (2%) or a Child (2%).

Figure 27 | *Victim of Identity Crime*

Business	*<1%*
Child	*2%*
Deceased	*1%*
Family	*2%*
Friend	*<1%*
Self	*92%*
Spouse/Partner	*2%*

Reports by Third Parties – Child

The primary type of identity crime reported that impacted children was False Employment (48%).

> **ADVISOR NOTES**
> *Caller reached out saying someone has been misusing her 1-year-old daughter's SSN for employment. The victim said she is unemployed and was informed when her benefits social worker requested documentation of her wages.*

The primary accounts impacted were IRS (30%), social media accounts (12%), credit card accounts (9%), checking accounts (9%) and medical insurance accounts (8%).

IRS accounts primarily involved someone fraudulently claiming a child on their taxes.

Social media accounts all involved ATO, while credit card, checking and medical insurance accounts primarily involved creating fraudulent new accounts using a child's PII.

Reports by Third Parties – Deceased

Reports of identity crimes involving a deceased individual's identity primarily involved a deceased parent (40%) or deceased spouse/partner (19%).

Identity crimes involving a deceased parent's account primarily involved existing ATO (60%), and identity crimes involving a deceased spouse's account primarily involved NAC (78%).

Reports by Third Parties – Spouse/Partner

Reports of identity crimes involving a spouse/partner primarily involved Scams (51%), NAC (20%) and Existing ATO (16%).

The primary scam type was Google Voice (68%), followed by a phony rental or purchase (9%) and phony business (6%).

NAC primarily involved credit cards (27%) and unemployment accounts (16%). Existing ATOs primarily involved credit cards (23%), checking accounts (20%) and social media accounts (20%).

Identity Criminal Profile

In most cases (91%), victims contacting the ITRC do not know who the identity criminal is.

Figure 28 | *Alleged Identity Criminals*

Unknown	*91%*
Other	*2%*
Ex-Spouse/Partner	*2%*
Family	*2%*
Friend	*1%*
Spouse/Partner	*1%*
Child/Dependent	*<1%*
Neighbor	*<1%*

In 84 percent (84%) of reported instances of identity misuse, the victims do not know the criminal.

Four percent (4%) of victims stated that the criminal in their misuse case(s) was their ex-spouse/ex-partner, and four percent (4%) of victims stated that the criminal in their misuse case(s) was a family member.

For crime being committed using a victim's PII, 85 percent (85%) of victims did not know the criminal, and nine percent (9%) of victims stated the criminal was a family member.

For new accounts created, 81 percent (81%) of victims did not know the criminal, six percent (6%) reported the bad actor was an ex-spouse or ex-partner, and six percent (6%) of victims stated the bad actor was a family member.

Most victims of identity compromise (95%) do not know who committed the identity crime against them.

For Lost or Stolen Items, 78 percent (78%) of victims do not know the criminal, four percent (4%) reported the criminal is their ex-spouse/ex-partner, four percent (4%) reported the criminal is a family member and four percent (4%) reported the thief is a child/dependent.

For unauthorized access to a computer/mobile device, 74 percent (74%) do not know the bad actor and nine percent (9%) indicated the bad actor was an ex-spouse/ex-partner.

2023 Identity Victimization Trends

- *Trend #1 – Improved Scams' Look and Message*
- *Trend #2 – More Severe Types of Identity Misuse*
- *Trend #3 – Thieves Already Have Enough Information*

Identity Victimization Trends

Trend #1 – Improved Scams' Look and Message

Identity thieves are improving at looking and sounding "legitimate", especially regarding job postings. It's probably generative AI-related.

In their constant efforts to thwart technological advances that help block threat actors, identity thieves continue to directly target victims in an effort to con individuals out of personal information. The same information identity criminals will sell or use to gain access to victims' individual, employer, business and government accounts.

In 2022 and early 2023, thieves primarily used victims' social media accounts to target not only victims but also victims' networks of family and friends. In 2023 and continuing into early 2024, we saw an increase in identity thieves creating phony job postings on legitimate networking and job search sites, enticing victims to apply for jobs. The bad actors created professional-looking LinkedIn profiles, or profiles on job sites, with live websites for phony businesses, or impersonated legitimate companies and used a fake name or a former employee's name to set up interviews.

Once a victim believed he/she/they had a legitimate request for an interview, the interview process was moved off the original platform to email, text, video conferencing platform, or a third-party messaging app. Victims were told they needed to fill out "paperwork" and provide proof of identity – either before or after they were offered a "job." Most victims did not think anything was strange – we are in a new era of remote work, and using technology to communicate is very normal. Providing sensitive personal information for identity verification (like a driver's license), proof of ability to work in the U.S. (like an SSN), and direct deposit information is part of the job onboarding process. It wasn't until after the victims shared their information and either did not hear from the company immediately after hearing from them very regularly or were asked to provide login information to ID.me that they became suspicious and contacted the ITRC.

The rapid improvement in the look, feel and messaging of identity scams is almost certainly the result of the introduction of AI-driven tools. A.I. tools help refine the "pitch" to make it more believable as well as compensate for cultural and grammar differences in language usage.

However, the primary defense against this advanced tech is effective and decidedly low-tech: pick up the phone and verify the contact directly from the source.

Trend #2 – More Severe Types of Identity Misuse

Victims are facing more severe types of identity misuse.

Not only are victims experiencing multiple types of identity misuse in multiple instances, but we continued to see an increase in the number of more severe types of identity misuse - victims whose SSN is being misused by someone to gain employment and victims whose information is being misused when someone else is convicted of a crime.

Identity crimes of this nature aren't as quickly discovered, take significant time to unravel and can require significant recovery time. They can also have a negative financial impact. Victims have reported being unable to obtain government benefits because of income reported that did not belong to them (or their children, in the many instances where victims only find out their, or their child's, SSN has been misused when they are being denied benefits).

Victims may also have been denied a refund from the IRS due to the income fraudulently tied to their SSNs. Victims who are required to have a background check are impacted when crimes they did not commit are attributed to them, often requiring significant investments in time and money they may not have to resolve the error.

Trend #3 – Thieves Already Have Enough Information

Identity thieves already have enough information to open new lines of credit and other accounts.

The widespread availability of personal information through data breaches, scams, and social media has created easy access for thieves to obtain and misuse the information. While cash is still preferred by criminals, identity thieves have found increasing success in using their victim's personal information to open lines of credit (or obtain other cash benefits) in their victims' names.

Reports of new, fraudulent credit cards, auto loans, mortgage loans and personal loans all increased in 2023 and continued into 2024, with many victims not finding out about the new obligations until the accounts went unpaid. As all victims of identity misuse know, the battle to prove that a person was a victim of a bad actor impersonating them.

Alliance for Identity Resilience (AIR) Advisory Board

The *Alliance for Identity Resilience* (AIR) was established as an advisory board by the Identity Theft Resource Center (ITRC). The advisory board operates within the framework of the ITRC's mission to empower individuals and businesses through education, support and innovative strategies. The primary purpose of AIR is to advise the ITRC on matters related to identity crime. The board serves as a consultative body to foster collaborative discussions, advance thought leadership and advocacy, identify emerging challenges, offer guidance on projects and initiatives, facilitate industry collaboration, and propose holistic solutions to enhance identity protection and victim recovery services.

Shawn Holtzclaw

Advisory Board Chair

Founder/Strategic Consultant,
Matrix Ventures, LLC

Jay Meier

Biometric Cohort Chair

SVP of North American Operations,
FaceTec, Inc.

Payam Hojjat

Advisor

Statewide Cybersecurity Risk & Governance
Chief, California Dept. of Technology

Meghan Land

Advisor

Executive Director,
Privacy Rights Clearinghouse

Cisa Kurian

Advisor

Principal Security Advisor (Lead Director)
Enterprise Information Security, CVS Health

Adam Levin

Advisor

Founder of CyberScout

Lynette Owens

Advisor

VP, Global Consumer Education & Product
Marketing, TrendMicro

Michael Scheumack

Advisor

Chief Innovations & Marketing Officer,
IDIQ

Stephen Smith

Advisor

SVP, Business & Strategy,
Intellectual Technology, Inc.

Arun Vemury

Advisor

Biometric & Digital Identity Technologist

About the Identity Theft Resource Center®

Founded in 1999, the Identity Theft Resource Center® (ITRC) is a national nonprofit organization established to empower and guide consumers, victims, business and government to minimize risk and mitigate the impact of identity compromise and crime. Through public and private support, the ITRC provides no-cost victim assistance and consumer education through its website live-chat idtheftcenter.org and toll-free phone number 888.400.5530. The ITRC also equips consumers and businesses with information about recent data breaches through its data breach tracking tool, *notified*. The ITRC offers help to specific populations, including the deaf/hard of hearing and blind/low vision communities.

2023 TRENDS IN IDENTITY REPORT

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT RESOURCE CENTER

AIR | ALLIANCE FOR IDENTITY RESILIENCE
ITRC ADVISORY BOARD

This report was made possible through the support of ***ITRC's Alliance for Identity Resilience (AIR) Advisory Board.***

Consumer & Business Resources

The ITRC offers a variety of low-cost identity education, protection, and recovery services for small businesses as well as free victim assistance and education opportunities for consumers. To learn more, email ***Dorinda Miller*** or contact the ITRC by email at ***communications@idtheftcenter.org***.

For Media

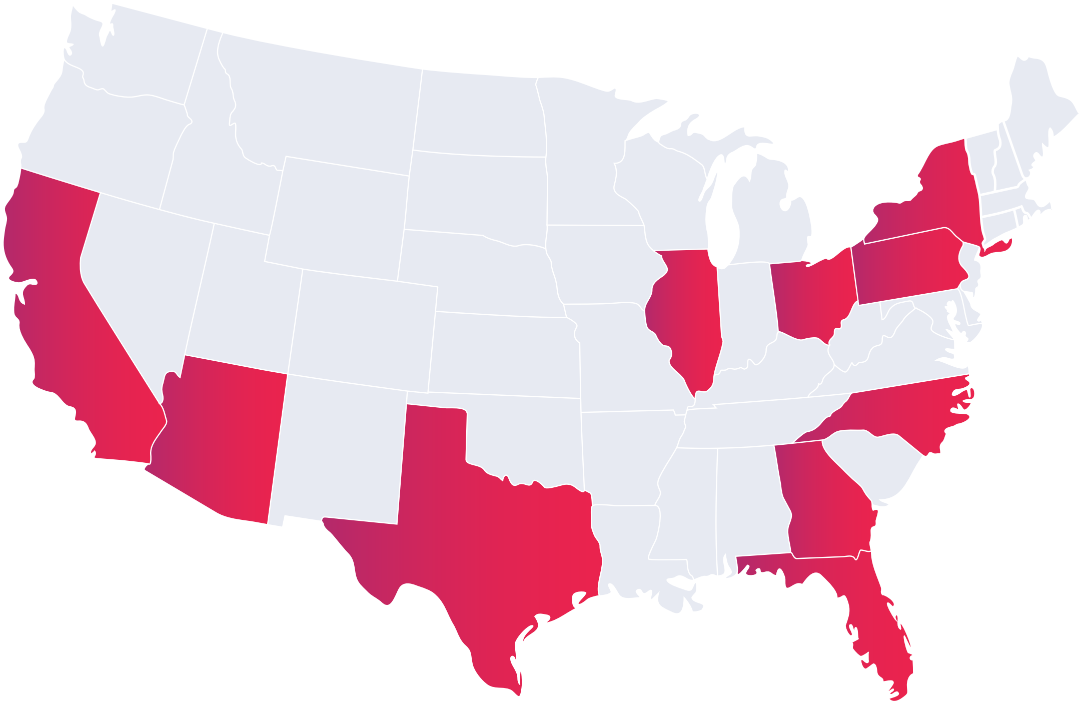
For any media-related inquiries, please email ***media@idtheftcenter.org***.

Appendix

+ Misuse by Type by State
+ Compromise by Type by State
+ Scam by State

Misuse by Type by State

Top 10 States by Total Victims Reporting Identity Misuse



Top 10 States by Total Victims Reporting Identity Misuse

1.	California	614
2.	Texas	282
3.	Florida	247
4.	New York	234
5.	Illinois	138
6.	Pennsylvania	122
7.	Ohio	113
8.	Georgia	111
9.	North Carolina	97
10.	Arizona	94

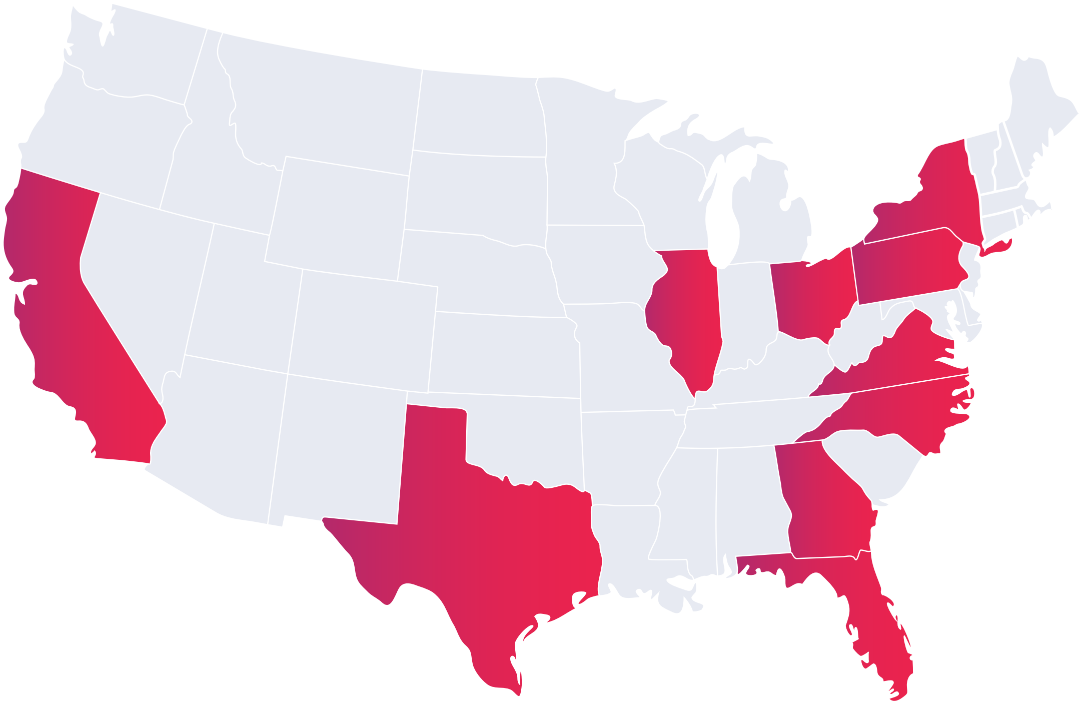
Victims Reporting Identity Misuse by Type by State

	Crime Committed Using Pii	Existing Account Takeover	False Employment	New Account Created	Other	State Totals
Alabama	5	33	0	19	0	57
Alaska	0	2	1	5	0	8
Arkansas	1	6	1	3	0	11
Arizona	6	27	23	38	0	94
California	31	298	54	229	2	614
Colorado	2	23	6	31	0	62
Connecticut	3	21	5	25	0	54
District of Columbia	3	3	0	6	0	12
Delaware	1	5	0	0	0	6
Florida	9	135	10	92	1	247
Georgia	4	54	5	45	3	111
Hawaii	1	9	0	2	1	13
Iowa	1	13	2	4	1	21
Idaho	0	5	1	9	0	15
Illinois	8	59	18	53	0	138
Indiana	6	31	0	20	0	57

	Crime Committed Using Pii	*Existing Account Takeover*	*False Employment*	*New Account Created*	*Other*	***State Totals***
Kansas	1	8	1	9	0	***19***
Kentucky	2	18	2	8	0	***30***
Louisiana	5	21	1	32	0	***59***
Massachusetts	5	34	4	32	1	***76***
Maryland	6	45	2	25	0	***78***
Maine	1	10	0	7	0	***18***
Michigan	1	47	0	33	0	***81***
Minnesota	3	18	1	17	0	***39***
Missouri	3	28	1	13	0	***45***
Mississippi	1	13	0	17	0	***31***
Montana	1	4	0	13	0	***18***
North Carolina	1	67	3	25	1	***97***
North Dakota	0	3	0	3	0	***6***
Nebraska	0	13	1	4	0	***18***
New Hampshire	0	12	0	2	0	***14***
New Jersey	3	49	2	34	1	***89***
New Mexico	8	16	6	41	2	***73***
Nevada	2	25	0	13	0	***40***
New York	6	128	9	90	1	***234***
Ohio	11	63	2	36	1	***113***
Oklahoma	1	13	3	19	0	***36***
Oregon	2	17	1	16	0	***36***
Pennsylvania	12	54	6	49	1	***122***
Rhode Island	1	2	0	1	0	***4***
South Carolina	1	32	1	22	0	***56***
South Dakota	0	4	0	0	0	***4***
Tennessee	5	45	1	28	0	***79***
Texas	23	121	30	106	2	***282***
Utah	0	3	5	10	0	***18***
Virginia	6	39	3	32	0	***80***
Vermont	0	4	0	1	0	***5***
Washington	2	41	2	23	0	***68***
Wisconsin	1	16	1	6	0	***24***
West Virginia	2	10	0	4	0	***16***
Wyoming	0	0	0	0	0	***0***
Totals	***197***	***1,747***	***214***	***1,352***	***18***	***3,528***

Compromise by Type by State

Top 10 States by Total Victims Reporting Identity Compromises



Top 10 States by Total Victims Reporting Identity Compromises

1.	*California*	***674***
2.	*Florida*	***382***
3.	*Texas*	***331***
4.	*New York*	***277***
5.	*Ohio*	***160***
6.	*Pennsylvania*	***158***
7.	*North Carolina*	***152***
8.	*Georgia*	***149***
	Illinois	***149***
10.	*Virginia*	***139***

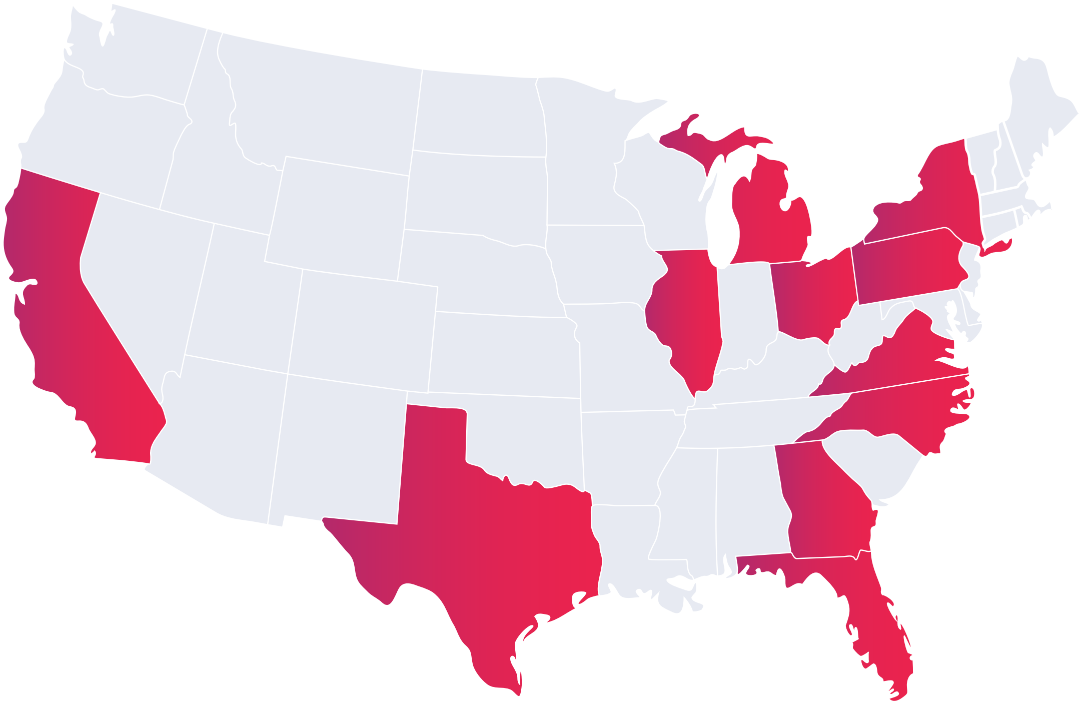
Victims Reporting Identity Compromises by Type by State

	Breach	*Impersonation*	*Mail Opened*	*Physical Items Lost/ Stolen*	*Picture of PII Docs Taken/Sent/Posted*	*PII Found on Dark Web*	*Scam*	*Unauthorized Access to Computer/Mobile Device*	*Other*	***State Totals***
Alabama	6	0	0	8	0	0	45	3	1	***63***
Alaska	1	1	0	0	0	0	7	0	0	***9***
Arkansas	1	0	0	0	0	0	11	1	0	***13***
Arizona	4	2	0	14	1	0	66	5	1	***93***
California	29	12	3	113	17	6	435	54	5	***674***
Colorado	3	1	3	10	2	1	84	10	0	***114***
Connecticut	2	0	1	2	2	0	33	6	0	***46***
District of Columbia	0	0	0	2	0	0	12	0	0	***14***
Delaware	0	0	0	1	1	0	13	0	0	***15***
Florida	8	8	1	34	7	1	288	31	4	***382***
Georgia	0	2	0	15	3	1	114	14	0	***149***
Hawaii	1	0	0	1	0	0	13	0	0	***15***
Iowa	0	0	0	2	0	0	21	1	0	***24***
Idaho	6	0	0	5	1	0	32	1	0	***45***
Illinois	5	3	0	9	1	1	118	11	1	***149***
Indiana	1	1	0	7	1	0	71	7	0	***88***

	Breach	Impersonation	Mail Opened	Physical Items Lost/ Stolen	Picture of PII Docs Taken/Sent/Posted	PII Found on Dark Web	Scam	Unauthorized Access to Computer/Mobile Device	Other	**State Totals**
Kansas	1	1	0	2	1	0	24	0	0	***29***
Kentucky	1	0	0	5	0	1	51	2	2	***62***
Louisiana	1	2	0	7	0	0	34	5	0	***49***
Massachusetts	6	2	0	4	1	2	80	9	0	***104***
Maryland	5	2	0	5	3	0	74	9	0	***98***
Maine	0	0	0	1	0	0	12	2	0	***15***
Michigan	5	3	0	10	1	1	109	5	0	***134***
Minnesota	3	1	0	4	0	0	71	4	1	***84***
Missouri	6	1	0	6	0	0	57	6	0	***76***
Mississippi	2	1	0	5	2	0	35	2	0	***47***
Montana	0	0	1	1	0	0	11	0	0	***13***
North Carolina	3	3	0	13	1	0	122	9	1	***152***
North Dakota	0	0	0	1	0	0	8	1	0	***10***
Nebraska	0	0	0	2	0	0	18	2	0	***22***
New Hampshire	3	2	0	1	0	0	22	3	0	***31***
New Jersey	4	3	0	11	0	1	110	2	1	***132***
New Mexico	3	1	0	13	0	0	27	0	1	***45***
Nevada	0	3	0	7	0	0	32	0	0	***42***
New York	6	5	1	25	2	6	208	23	1	***227***
Ohio	1	3	0	9	3	0	136	6	2	***160***
Oklahoma	1	1	1	2	0	0	50	5	0	***60***
Oregon	6	1	0	6	2	1	43	3	0	***62***
Pennsylvania	8	4	0	4	4	2	122	12	2	***158***
Rhode Island	0	0	0	0	0	0	11	0	0	***11***
South Carolina	2	3	1	4	2	0	44	7	0	***63***
South Dakota	1	0	0	0	0	0	9	0	0	***10***
Tennessee	3	3	0	0	1	0	63	3	0	***73***
Texas	17	6	0	43	5	2	232	23	2	***331***
Utah	1	1	0	2	1	0	32	2	0	***39***
Virginia	8	1	0	9	0	2	109	9	1	***139***
Vermont	0	0	0	0	0	0	9	0	0	***9***
Washington	5	2	0	7	4	1	66	8	1	***94***
Wisconsin	3	2	0	1	1	0	67	2	0	***76***
West Virginia	1	1	0	1	0	0	20	0	0	***23***
Wyoming	0	0	0	0	1	0	6	1	0	***8***
Totals	***238***	***113***	***18***	***577***	***115***	***39***	***5,451***	***434***	***44***	***7,029***

Scam by State

Top 10 States by Total Victims Reporting Identity Scam



Top 10 States by Total Victims Reporting Identity Scam	
1. California	447
2. Florida	293
3. Texas	237
4. New York	212
5. Ohio	132
6. Pennsylvania	131
7. North Carolina	123
8. Illinois	118
9. Georgia	115
10. Michigan	112
Virgina	112

Victims Reporting Identity Scam by State

	Google Voice	Job/ Employment	Phony Business/ Organization	Phony Government Agency	Phony Financial	Phony Law Enforcement	Lottery/Prize	Unknown	Romance/ Sweetheart	Rental/Purchase	Tech Support	Government Grant	Other	State Totals
Alabama	23	3	3	2	0	0	7	3	0	0	1	1	0	*43*
Alaska	3	0	2	1	0	0	0	0	0	0	0	0	0	*6*
Arkansas	7	1	1	0	0	0	1	1	0	0	0	0	0	*11*
Arizona	43	6	6	1	2	1	4	0	2	1	2	0	0	*68*
California	224	33	48	21	23	5	5	15	21	18	6	13	5	*447*
Colorado	52	3	4	7	6	2	2	1	1	3	5	1	1	*88*
Connecticut	24	2	0	2	1	0	3	0	0	0	2	0	0	*34*
District of Columbia	9	0	1	0	0	0	0	0	0	0	1	0	1	*12*
Delaware	6	3	0	1	1	0	1	1	0	0	0	0	0	*13*
Florida	193	18	21	13	5	1	16	8	3	7	2	3	3	*293*
Georgia	78	9	4	3	2	1	6	3	5	2	0	2	0	*115*
Hawaii	7	0	0	2	1	0	0	0	0	0	0	1	1	*12*
Iowa	16	0	2	2	0	0	3	0	0	0	0	0	0	*23*
Idaho	16	4	4	2	2	0	2	0	1	1	1	0	0	*33*
Illinois	77	5	4	6	1	0	6	5	2	3	4	3	2	*118*
Indiana	47	6	3	5	3	1	3	2	2	0	2	0	0	*74*

	Google Voice	Job/ Employment	Phony Business/ Organization	Phony Government Agency	Phony Financial	Phony Law Enforcement	Lottery/Prize	Unknown	Romance/ Sweetheart	Rental/Purchase	Tech Support	Government Grant	Other	State Totals
Kansas	17	1	2	0	0	1	1	1	1	2	0	1	0	*27*
Kentucky	27	5	6	3	1	0	6	2	2	0	0	1	0	*53*
Louisiana	21	1	1	2	0	0	1	4	3	2	0	0	0	*35*
Massachusetts	60	0	3	3	3	0	1	1	2	0	5	1	0	*79*
Maryland	38	5	10	1	2	1	6	4	2	2	1	1	1	*74*
Maine	6	0	1	0	0	0	1	0	0	2	3	0	0	*13*
Michigan	79	3	9	2	0	1	5	5	2	1	2	2	1	*112*
Minnesota	47	6	7	3	1	0	5	2	0	0	0	1	0	*72*
Missouri	40	1	7	0	1	0	2	1	2	1	1	0	1	*57*
Mississippi	17	3	2	3	0	1	7	1	0	1	0	1	0	*36*
Montana	6	0	1	0	1	0	3	0	0	0	0	0	0	*11*
North Carolina	69	9	12	3	6	0	11	2	3	2	2	1	3	*123*
North Dakota	7	0	0	0	0	0	0	0	1	0	0	0	0	*8*
Nebraska	13	0	2	0	0	0	2	2	0	0	0	0	0	*19*
New Hampshire	17	0	2	1	0	0	2	0	0	0	0	1	0	*23*
New Jersey	70	7	6	4	5	0	2	3	1	5	3	1	2	*110*
New Mexico	13	3	2	4	0	0	5	1	0	0	0	0	0	*28*
Nevada	15	0	4	1	4	1	5	1	0	0	1	0	2	*34*
New York	113	19	20	11	6	1	18	7	4	4	3	3	3	*212*
Ohio	80	10	7	4	2	0	12	4	5	3	0	4	1	*132*
Oklahoma	21	6	3	0	0	0	11	3	2	1	0	3	0	*50*
Oregon	34	3	2	1	0	1	3	0	0	0	0	0	0	*44*
Pennsylvania	90	3	8	6	2	0	9	3	1	2	4	1	2	*131*
Rhode Island	10	0	0	0	0	0	0	2	0	0	0	0	0	*12*
South Carolina	25	2	3	2	2	1	1	2	4	0	1	1	0	*44*
South Dakota	6	0	2	0	0	0	0	1	0	0	0	0	0	*9*
Tennessee	35	5	7	2	3	0	5	1	3	2	1	1	11	*66*
Texas	133	27	17	7	3	0	19	7	9	6	5	3	1	*237*
Utah	21	2	1	2	0	0	2	1	1	0	1	1	1	*33*
Virginia	79	2	5	5	4	0	6	2	1	6	2	0	0	*112*
Vermont	7	1	0	0	1	0	0	0	0	0	0	0	0	*9*
Washington	36	5	8	4	0	1	9	3	3	1	1	0	0	*71*
Wisconsin	55	1	1	4	0	0	4	0	1	1	0	1	0	*68*
West Virginia	9	2	1	0	0	1	4	2	0	0	1	0	1	*21*
Wyoming	3	1	0	0	0	0	0	0	0	2	0	0	0	*6*
Totals	***3,414***	***492***	***204***	***114***	***55***	***21***	***307***	***117***	***112***	***111***	***79***	***76***	***53***	***5,215***