TIR

IDENTITY THEFT RESOURCE CENTER

2025 Trends in Identity Report

ALLIANCE FOR IDENTITY RESILIENCE
ITRC ADVISORY BOARD

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

ITRC | IDENTITY THEFT RESOURCE CENTER

JUNE 2025

CONTENTS

IDENTITY CONCERNS

APPENDIX

INTRODUCTION

from the COO & Head of Victim Services

The *Trends in Identity Report* (TIR) is based on the issues facing the people who contact the Identity Theft Resource Center (ITRC) every day. Most are victims of identity theft, fraud or scams, but not all, as more people actively take personal responsibility for protecting their information.

One macro trend that has carried over from 2023 into 2024 (and continues this year) is a decline in the number of victims reporting crimes. Fewer people are reporting identity crimes but those who do suffer greater financial losses. The ITRC, the Federal Trade Commission and the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) have all reached the same conclusion as to what is happening. However, there is no consensus as to why this is happening. Some of the reasons include:

+ Criminals are using technology like artificial intelligence (AI) to target victims more precisely, so they don't need to attack as many people, but those they do attack lose more money.
+ "Victim fatigue" associated with the unrelenting pace of data breaches and cyberattacks has created a sense of hopelessness and powerlessness.
+ More people are taking personal responsibility for protecting their identity information, and more organizations are deploying tools that effectively block or minimize attacks.

This year's TIR also gives us a snapshot of what we can expect in the year ahead. In particular, we see three trends driving the behavior of professional identity criminals who commit theft, fraud and scams, and the outcomes of their crimes.

1. AI is having an impact.
2. It's never been easier to take over someone's accounts.
3. People are taking steps to protect themselves in ways and rates they have not previously.

In this report, we make a distinction between a crime victim and someone who is seeking prevention information. We use terms like ***compromise*** and ***misuse***.

> ***Compromise*** is when an individual's information has been exposed, like through a data breach, or shared with a bad actor. When a compromise is reported, the victim's information has not been knowingly misused.
>
> ***Misuse*** describes when a victim knows a bad actor has fraudulently used their personal information to open a new account, take over an existing account or even evade a crime, for example. At this point, victims need a recovery plan.

This report also includes what information was sought and how it was used (or intended to be misused) by a criminal. Many bad actors are using impersonation scams and job scams, among others, to obtain sensitive information like Social Security numbers and driver's license information, while others are stealing actual Social Security cards and driver's licenses. They typically use that information to take over bank accounts and social media accounts and open new credit card accounts.

What you won't see is a discussion of the financial, emotional and physical impacts of the identity theft, fraud and scams described here. That will be covered in the ITRC's *2025 Consumer & Business Impact Report*, published in October.

However, this data reinforces an important point. Gone are the days when only certain people or businesses were the target of identity criminals. Everyone can be a victim today, but there are ways to prevent becoming a victim and recover when you do – it all starts with a call to the ITRC.

Mona Terry
COO & Head of Victim Services, Identity Theft Resource Center

GLOSSARY

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 developed 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, but has not yet been misused.

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 identity fraud (open accounts, take over accounts, commit a crime, obtain employment, etc.).

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

New Account Fraud – Opening new credit card or bank accounts using stolen personally identifiable information (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).

TRENDS

TREND #1

Artificial Intelligence (AI) technology makes it easier for thieves to coerce unsuspecting victims into giving away their identity credentials.

Sharing personal information in a scam continues to be the primary method of identity compromise reported to the ITRC. Tactics used to lure victims into a scam include using AI to spoof legitimate websites, posting ads on search engines with fake customer service numbers for well-known businesses or sending legitimate-looking emails that pretend to be from a large company. They also send text messages that seem to come from legitimate sources. AI tools allow scammers to operate on a much larger scale and target more victims efficiently.

As AI-generated content becomes more realistic, it becomes more difficult to identify and block fraudulent attempts. And the thieves don't just ask for money. They will work to get as many personal identifiers as possible to take over accounts, establish new ones or sell the information to make money.

TREND #2

Identity thieves are increasingly able to access a variety of existing accounts.

This latest reporting period has shown an increase in account takeovers and new types of account compromises. Identity thieves are increasingly targeting individuals' phones.

They also target identity verification platforms by tricking victims into sharing their account information or allowing account access once their identity has been verified. The interconnected nature of today's digital services means that access to one account can provide a pathway to others, making identity crimes more damaging and far-reaching.

Victims aren't the only source of information. Businesses continue to be plagued by data breaches, allowing victims' information to get into the hands of bad actors. Thieves now have enough information to convince victims that they are from a legitimate source and entice the remaining pieces of personal data they need to take over a victim's accounts.

TREND #3

Individuals are becoming more curious about protecting their identity.

As threats become more visible and widespread, more individuals no longer rely on account issuers to protect their information or to actively notify them of fraudulent use of their identity. Public awareness is growing, fueled by news reports and firsthand experiences with fraud. The ITRC has seen an increase in individuals actively seeking to protect their information or investigating suspicious activity before becoming victims of identity theft, scams or fraud.

TIR

IDENTITY THEFT RESOURCE CENTER

2025 Trends in Identity Report

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. *All data is based on individuals who contacted the ITRC 4/1/24 – 3/31/25.*

ITRC | IDENTITY THEFT RESOURCE CENTER

TOTAL CRIMES REPORTED

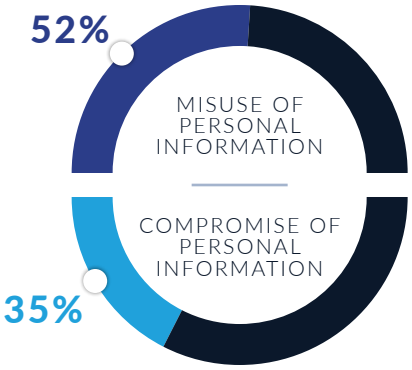
9,038

Q2 2024 THROUGH Q1 2025

NEW CASES REPORTED

Decreased 31 Percentage Points

FROM 2023



CRIMES REPORTED

TO THE ITRC

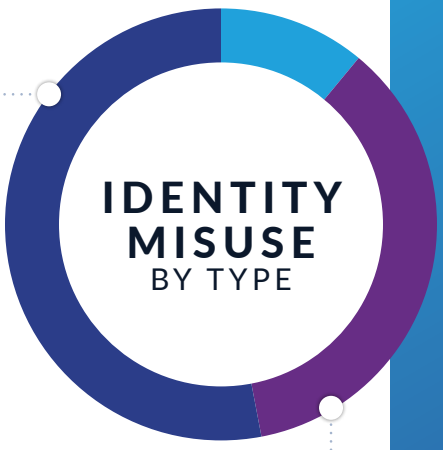
*In previous years, **more victims reported compromise** of their personal information than misuse.*

TOP 3 REASONS FOR CONTACTING THE ITRC

UNRELATED TO COMPROMISE OR MISUSE

- **29%** *UNSURE IF A VICTIM OF MISUSE*
- **29%** *SCAM VICTIM – PII NOT SHARED*
- **14%** *PREVENT IDENTITY THEFT*

Checking bank account (22%) was the most reported type of existing account takeover.



- *Account Takeover **53%***
- *New Account Creation **36%***
- *Other **11%***

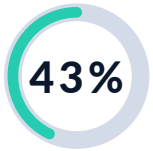
*The most reported type of new accounts being created was **credit card accounts (30%).***

- ***76%** One Incidence*
- ***14%** Two Incidences*
- ***6%** Three Incidences*
- ***4%** Four of More Incidences*

*The number of people experiencing multiple identity-related incidences **increased from 15% to 24%** year-over-year.*

IDENTITY COMPROMISES

BY TYPE



TOP IDENTITY COMPROMISE

Scam Where Victim's PII Was Shared

TOP 3 SCAMS REPORTED

***Impersonation** – 34%*
***Job/Employment** – 10%*
***Google Voice** – 9%*

IDENTITY VICTIMIZATION TRENDS

IDENTIFIED BY THE ITRC

TREND #1

Artificial Intelligence (AI) technology makes it easier for thieves to coerce unsuspecting victims into giving away their identity credentials.

TREND #2

Identity thieves are increasingly able to access various existing accounts.

TREND #3

Individuals are becoming more curious about protecting their identity.

AIR | ALLIANCE FOR IDENTITY RESILIENCE
ITRC ADVISORY BOARD

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

IDENTITY CONCERNS

REQUESTS REGARDING IDENTITY-RELATED CONCERNS

ATTEMPTED MISUSE OF IDENTITY CREDENTIALS

IDENTITY COMPROMISE

Scams

IDENTITY MISUSE

Accounts

IRS

IDENTITY CONCERNS

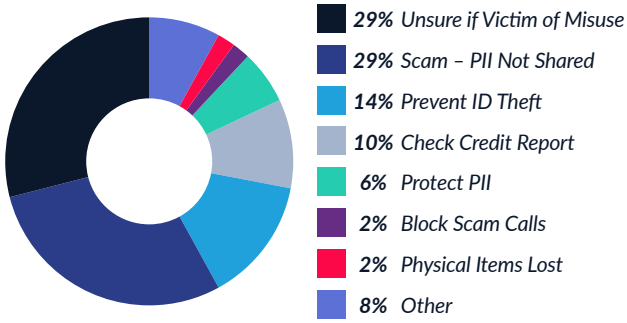
Individuals contacting the ITRC primarily reported misuse of their personal information (52%), followed by personal information compromised (35%), wanting identity-related or preventative information (11%) and attempted misuse of personal information (3%).

This is a shift from prior years when more victims reported being victims of personal information compromise (50%) than misuse (41%).

REQUESTS REGARDING IDENTITY-RELATED CONCERNS

Individuals who contacted the ITRC about an identity-related concern, whose information had not been compromised or misused, primarily did so because they were contacted by a scammer (29%) and were concerned about the information the criminal already had about them. They were not sure if their information had been misused (29%), but were concerned that it may have been. Other concerns involved individuals wanting to know how to prevent identity theft (14%) and needing assistance checking their credit report (10%).

Figure 1 | *Contacted ITRC About Identity-Related Concern*



ATTEMPTED MISUSE OF IDENTITY CREDENTIALS

Attempted misuse of identity credentials occurred when a thief attempted to open a new account or take over an existing account of a victim, but was unsuccessful. The account issuer typically notified victims that they were subjected to attempted identity misuse.

Similar to the prior reporting period, victims primarily reported attempted misuse of their identity credentials when the thief tried to open a new account (69%) versus attempted takeover of an existing account (31%).

Attempted misuse largely involved financial accounts (85%), specifically credit card accounts (56% of reported accounts) and checking accounts (14% of reported accounts).

Figure 2 | *Attempted Misuse by Account Type*

Type of Account	Percentage	Type of Account	Percentage
Credit Card	56%	Personal Tech Account	2%
Checking Account	14%	Mortgage Loan	1%
Personal Loan	6%	Unemployment	1%
Auto Loan	3%	Property Lease/Rental	1%
IRS	2%	SNAP/Food Stamps	1%
Investment	2%	CRA	1%
Payday Loan	2%	Phone	1%
Insurance – Medical	2%	Other	8%

"[The] 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."

"The calls I had to make, sometimes waiting on hold for hours to talk to the right people. It was miserable, and waiting to find out from them if I was hacked or not. My issue has not been resolved yet because they still have my information. They still have my driver's license with my information. I don't trust anyone. When I make a purchase, I live in fear until everything clears. Then, I check my account regularly for a long time afterward. I feel like everyone is a threat."

IDENTITY COMPROMISE

Similar to the prior reporting period, the top methods of identity compromise reported to the ITRC were due to PII being shared in a scam, stolen documents with personal information and unauthorized access to a computer or mobile device.

Notably, there was a 41 percent (41%) decrease in victims reporting their PII was shared in a scam. However, there was an overall increase in other reported compromises, including a 71 percent (71%) increase in reports of stolen documents with personal information.

Trend We're Watching:

+ Reports of unauthorized computer or mobile device access increased by 104 percent (104%) (7% of reports in 2023-2024 vs. 15% of reports in 2024-2025).

Figure 3 | *Compromise by Type, Year-Over-Year*

	2024 – 2025	2023 – 2024	Change
Scam – PII Shared	43%	73%	-41%
Physical Items Stolen	17%	10%	71%
Unauthorized Access to Computer/Mobile	15%	7%	104%
Breach	14%	4%	235%
PII Found on Dark Web	6%	1%	865%
Impersonation	3%	2%	18%
Picture of PII Doc Taken/Sent/Posted	1%	2%	-22%
Mail Opened	1%	0%	84%
Other	0%	1%	-29%

Individuals who reported stolen documents with personal information primarily reported stolen driver's licenses, Social Security cards, payment cards, birth certificates and phones or tablets.

Trend We're Watching:

+ There was a 612 percent (612%) increase in reports of birth certificates stolen (1% of reports in 2023-2024 vs. 8% of reports in 2024-2025).

Figure 4 | *Stolen Documents or Items Reported, Year-Over-Year*

	2024 – 2025	2023 – 2024	Change
Driver's License/State ID	22%	20%	8%
Social Security Card	20%	18%	10%
Payment Card(s)	13%	2%	475%
Birth Certificate	8%	1%	612%
Phone/Tablet	6%	5%	18%
Medical Insurance Card	3%	1%	359%
Passport	3%	2%	31%
Checkbook/Checks	2%	0%	654%
Documents – Tax	2%	3%	-19%
Mail	2%	–	–
Payment/Refund Check	1%	0%	261%
Stimulus Payment	1%	3%	-77%
Laptop	1%	1%	-13%
Documents – Auto Registration/Title	0%	2%	-73%
Documents – Other	7%	16%	-59%
Other	9%	25%	-62%

"The barriers are 22 years of my life – being flagged for fraud, being refused information because nobody knew if I did something – or if I was myself. I ended up absolutely destroying my life at 46, filing for bankruptcy to get rid of all the collections that weren't mine. And when I rebuilt, I had my accounts closed for fraud because they didn't know if I was me or she was me. My entire life was destroyed. How can I fix 22 years? It can't be done."

SCAMS

Similar to last year, the top three scams reported to the ITRC were: impersonation, job/employment and Google Voice.

Trends We're Watching:

- Impersonation scams grew 148 percent (148%) year-over-year.
  - Scammers typically impersonated a business (51 percent (51%) of impersonation scams) or a financial institution (21%), with increased reports of impersonation in both categories. While the next highest category of impersonation was a federal/state agency, there was a 32 percent (32%) decrease in reports of impersonation of a government agency compared to the same timeframe in the previous year.
  - Business impersonation primarily involved spoofed emails and internet searches for companies that led to fraudulent customer service numbers and/or websites, while financial impersonation largely involved inbound calls to victims.
- New types of scams reported to the ITRC included toll road scams, which accounted for three (3) percent (3%) of all reported scams.

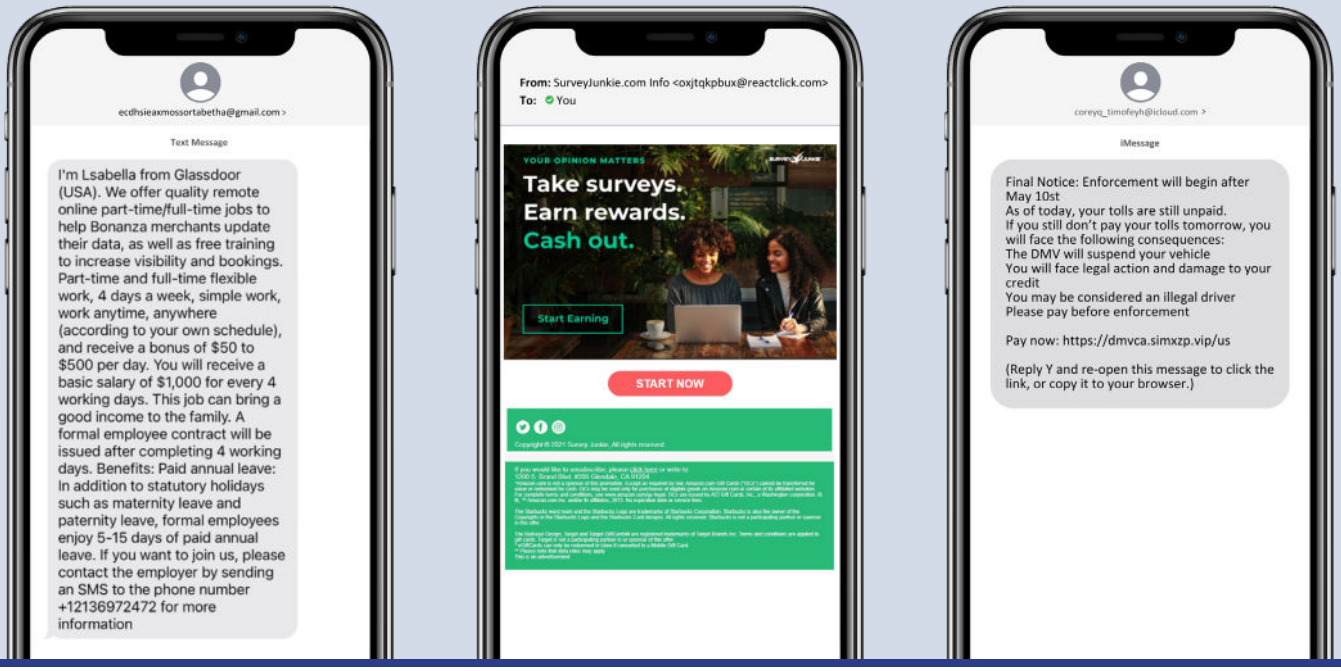
Figure 5 | *Type of Scam, Year-Over-Year*

	2024 – 2025	2023 – 2024	Change
Impersonation	34%	14%	148%
Job/Employment	10%	14%	-31%
Google Voice	9%	54%	-84%
Lottery/Prize	8%	3%	143%
Rental/Purchase (Home, Pet, Car, etc.)	4%	2%	116%
Tech Support	4%	2%	98%
Cryptocurrency	4%	1%	503%
Romance	3%	2%	62%
Toll Road	3%	–	–
Grant	2%	2%	44%
Other	12%	4%	20%
Unknown	7%	2%	225%

Figure 6 | *Type of Impersonation Scam, Year-Over-Year*

	2024 – 2025	2023 – 2024	Change
Business	51%	48%	5%
Financial Institution	21%	19%	10%
Federal/State Agency	19%	29%	-32%
Police/Sheriff	3%	3%	0%
Friend/Family	2%	1%	377%
Celebrity	1%	–	–
Charity	1%	–	–
Employer	1%	1%	-11%
Foreign Embassy	0%	0%	-100%
Unknown	1%	–	–

EXAMPLES OF SCAMS



Personal information obtained by the scammer can consist of sensitive or non-sensitive personal information.

The most common pieces of non-sensitive personal information obtained by the scammer included name (25%), phone number (15%) and address (14%).

The most common pieces of sensitive personal information obtained by the scammer included Social Security number (9%), driver's license number (7%), payment card number (4%) and account number (4%).

Figure 7 | *Type of PII Involved in a Scam, Year-Over-Year*

	2024 – 2025	2023 – 2024	Change
Name	25%	23%	8%
Phone Number	15%	29%	-46%
Address	14%	10%	40%
Date of Birth	9%	8%	20%
Social Security Number (Full, Partial)	9%	7%	17%
Driver's License Number	7%	6%	8%
Email Address	5%	5%	6%
Payment Card Number	4%	2%	139%
Account Number	4%	3%	65%
Picture	3%	4%	-18%
Passport	1%	1%	67%
Username (Login)	1%	1%	-15%
Passport Number	1%	1%	-8%
Other	2%	–	–

"Financial identity theft can ruin you if not prepared. I have been homeless and hungry more days and nights than I care to ever see again."

IDENTITY MISUSE

Most reported misuse involved misuse of accounts, including account takeover (53%) and new accounts created using an individual's personal information (36%). Victims also reported misuse related to fraudulent employment (6%), crimes committed using the victim's personal information (4%) and IRS misuse (4%).

Trends We're Watching:

+ Reports of fraudulent employment are up three (3) percent (3%) year-over-year, and the ITRC has seen an upward trend in reports of fraudulent employment in Q1 2025.
+ There was an 11 percent (11%) increase in reports of existing account takeover.

Figure 8 | *Misuse by Type, Year-Over-Year*

	2024 – 2025	2023 – 2024	Change
Account Takeover	53%	47%	11%
New Account Created	36%	37%	-4%
Fraudulent Employment	6%	5%	3%
Crime Committed Using PII	4%	5%	-9%
IRS Misuse	4%	4%	-5%
Other	1%	1%	-29%

"I was so glad I found your advisor to help me. Victims of crimes like this have to make a choice to look for help or just bury it because of shame. The advisor didn't make me feel like he/she was judging me or that I was stupid for being taken in by this scam. The questions asked were easy to answer and those answers made me see what a scam this was. I was open to any advice that was given and plan to follow through with exposing this for what it is."

ACCOUNTS

Reports of account misuse involved financial accounts (52%), other accounts (35%), federal (non-IRS) accounts (7%) and state accounts (6%).

The majority of accounts reported as misused were credit card accounts (23 percent (23%) of accounts), checking accounts (17 percent (17%) of accounts) and social media accounts (15 percent (15%) of accounts).

Following the overall trend for accounts, account takeover primarily impacted checking accounts (22 percent (22%) of accounts taken over), social media accounts (19%) and credit card accounts (17%).

Trends We're Watching:

+ There was a 754 percent (754%) increase in reports of account takeover involving personal tech accounts (Apple, Google, etc.).
+ There was a 47 percent (47%) increase in reports of account takeover involving person-to-person payment apps (Venmo, Zelle, etc.).
+ There were no reports of account takeover in 2023-2024 vs. 31 reports in 2024-2025.

Figure 9 | *Existing Account Takeover, Year-Over-Year*

	2024 – 2025	2023 – 2024	Change
Bank – Checking	22%	22%	1%
Social Media	19%	25%	-25%
Credit Card	17%	16%	4%
Email	7%	6%	8%
Personal Tech Account	4%	0%	754%
P2P Payment App	3%	2%	47%
Utility – Phone	3%	3%	-4%
Email – Personal	2%	2%	18%
CRA	2%	1%	26%
Merchant	2%	1%	35%
Insurance – Medical	2%	1%	7%
DMV	1%	1%	11%
ID.me	1%	–	–
Investment	1%	1%	10%
Banking – Savings	1%	1%	91%
SNAP/Food Stamps	1%	1%	32%
SSA –Disability	1%	1%	-32%
SSA – Medicare	0%	1%	-22%
Unemployment	0%	1%	-29%
Mail	0%	1%	-66%
Other	11%	13%	-15%

Reports of fraudulent new accounts centered around credit card accounts (30 percent (30%) of fraudulent new accounts), checking accounts (11%), auto loans (6%) and personal loans (6%).

Trends We're Watching:

+ There was a 102 percent (102%) increase in fraudulent new property leases/rentals reports.
+ There was a 111 percent (111%) increase in reports of fraudulent federal student loans.

Figure 10 | *New Account Creation, Year-Over-Year*

	2024 – 2025	2023 – 2024	Change
Credit Card	30%	32%	-5%
Banking – Checking	11%	10%	8%
Auto Loan	6%	5%	6%
Personal Loan	6%	6%	-10%
Mortgage Loan	5%	6%	-24%
Utility – Phone	4%	4%	-2%
Unemployment	4%	6%	-38%
Property Lease/Rental	3%	1%	102%
Medical Provider	3%	2%	37%
SBA	2%	2%	9%
DMV	2%	1%	18%
Insurance – Medical	2%	3%	-42%
Student Loan – Federal	2%	1%	111%
P2P Payment App	1%	1%	1%
Utility – Electricity	1%	1%	5%
SNAP/Food Stamps	1%	1%	40%
Social Media	1%	1%	24%
Payday Loan	1%	1%	100%
ID.me	1%	0%	1,690%
Student Loan – Private	1%	1%	20%
Investment	1%	1%	22%
Business EIN	1%	1%	13%
Merchant	1%	1%	-12%
Insurance – Auto	1%	1%	34%
Utility – Internet	1%	1%	-3%
State Department of Revenue	1%	0%	65%
CRA	1%	0%	45%
Insurance – Other	1%	0%	58%
Utility – Cable	0%	1%	-47%
Medicaid	0%	1%	-53%
Other	8%	8%	0%

IRS

In prior years, IRS Misuse was categorized as Federal Account Misuse. However, given the unique nature of the concerns victims face with their IRS account, identity misuse regarding IRS accounts has been given its own category.

Victims primarily report taxes being filed in their name (59%), an individual or child/children being fraudulently claimed as a dependent (15%), not receiving a tax credit or stimulus payment due to identity concerns (4%), contact or bank information changed in their account (3%) or other misuse concerns (19%).

ADVISORY BOARD

Alliance for Identity Resilience (AIR)

The *Alliance for Identity Resilience* (AIR) was established as an advisory board by the 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.

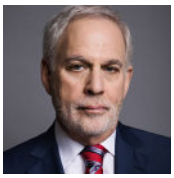
JAY MEIER
Biometric Cohort Chair
President & CEO – Sage Capital Advisors, LLC.

STEVE CRAIG
Advisor
Founder, CEO – PEAK IDV

PAYAM HOJJAT
Advisor
Cybersecurity Risk & Governance Chief – State of California / Cybersecurity Professor – California State University

CISA KURIAN
Advisor
Lead for Consumer Identity & Access Management (CIAM) – CVS Health

MEGHAN LAND
Advisor
Executive Director – Privacy Rights Clearinghouse (PRC)



ADAM LEVIN
Advisor
Chairman & Founder – CyberScout

AARON MENDES
Advisor
CEO & Co-Founder – PrivacyHawk

LYNETTE OWENS
Advisor
Vice President, Global Consumer Education & Product Marketing – Trend Micro

LISA PLAGGEMIER
Advisor
Executive Director – National Cybersecurity Alliance

MICHAEL SCHEUMACK
Advisor
Chief Marketing & Innovation Officer – IDIQ

STEPHEN SMITH
Advisor
Senior Vice President, Business & Strategy – Intellectual Technology (ITI)

TIR

IDENTITY THEFT RESOURCE CENTER

2025 Trends in Identity Report

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 at Dorinda@idtheftcenter.org or contact the ITRC by email at communications@idtheftcenter.org.

FOR MEDIA

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

CONTRIBUTORS

Thanks to the team responsible for the *2025 ITRC Trends in Identity Report*:

Analysis & Editorial – Mona Terry
Layout & Design – Meagan Lechleiter

AIR | ALLIANCE FOR IDENTITY RESILIENCE
ITRC ADVISORY BOARD

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

ITRC | IDENTITY THEFT RESOURCE CENTER

JUNE 2025

APPENDIX

VICTIMS BY STATE

MISUSE BY STATE

Top 10 States By Total VIctims

Misuse By Type

COMPROMISE BY STATE

Top 10 States By Total VIctims

Compromise By Type

CONTACTS TO THE ITRC

DEMOGRAPHIC DATA

Age

Ethnicity

Income

Gender

Specific Populations

Victim vs. Thief

VICTIMS
By State

Based on victims who shared their state of residence:

Top 10 States

Reported State of Residence	Percentage
California (CA)	28%
Texas (TX)	10%
Florida (FL)	8%
New York (NY)	8%
North Carolina (NC)	5%
Illinois (IL)	4%
Pennsylvania (PA)	4%
Arizona (AZ)	4%
Ohio (OH)	4%
Georgia (GA)	3%

Reports of Misuse

Following nationwide trends, the states with the highest instances of misuse primarily reported misuse of accounts through account takeover or the establishment of new accounts.

Residents of AZ and IL reported markedly higher percentages of fraudulent employment.

Reports of Misuse by Top 10 States

	Crime Committed Using PII	Existing Account Takeover	Fraudulent Employment	IRS Misuse	New Account Created	**Total Reports of Misuse**
CA	5%	43%	9%	4%	37%	**16%**
TX	4%	39%	8%	8%	42%	**5%**
FL	4%	50%	1%	1%	42%	**4%**
NY	4%	57%	4%	4%	31%	**4%**
IL	1%	41%	17%	3%	38%	**2%**
NC	6%	57%	0%	1%	34%	**2%**
AZ	6%	23%	29%	6%	35%	**2%**
PA	3%	43%	8%	4%	43%	**2%**
OH	4%	46%	6%	5%	35%	**2%**
GA	7%	42%	6%	1%	43%	**2%**

Reports of Compromise

Following nationwide trends, the states with the highest instances of compromised personal information primarily reported that their information was compromised in a scam, due to stolen documents containing personal information and unauthorized access to a computer or mobile device.

Residents in NC and IL reported the most significant percentage of compromise due to a breach.

Residents in CA and FL reported the largest percentage of compromise due to stolen documents with personal information.

Residents in TX reported the highest percentage of compromises due to unauthorized access to a computer or mobile device.

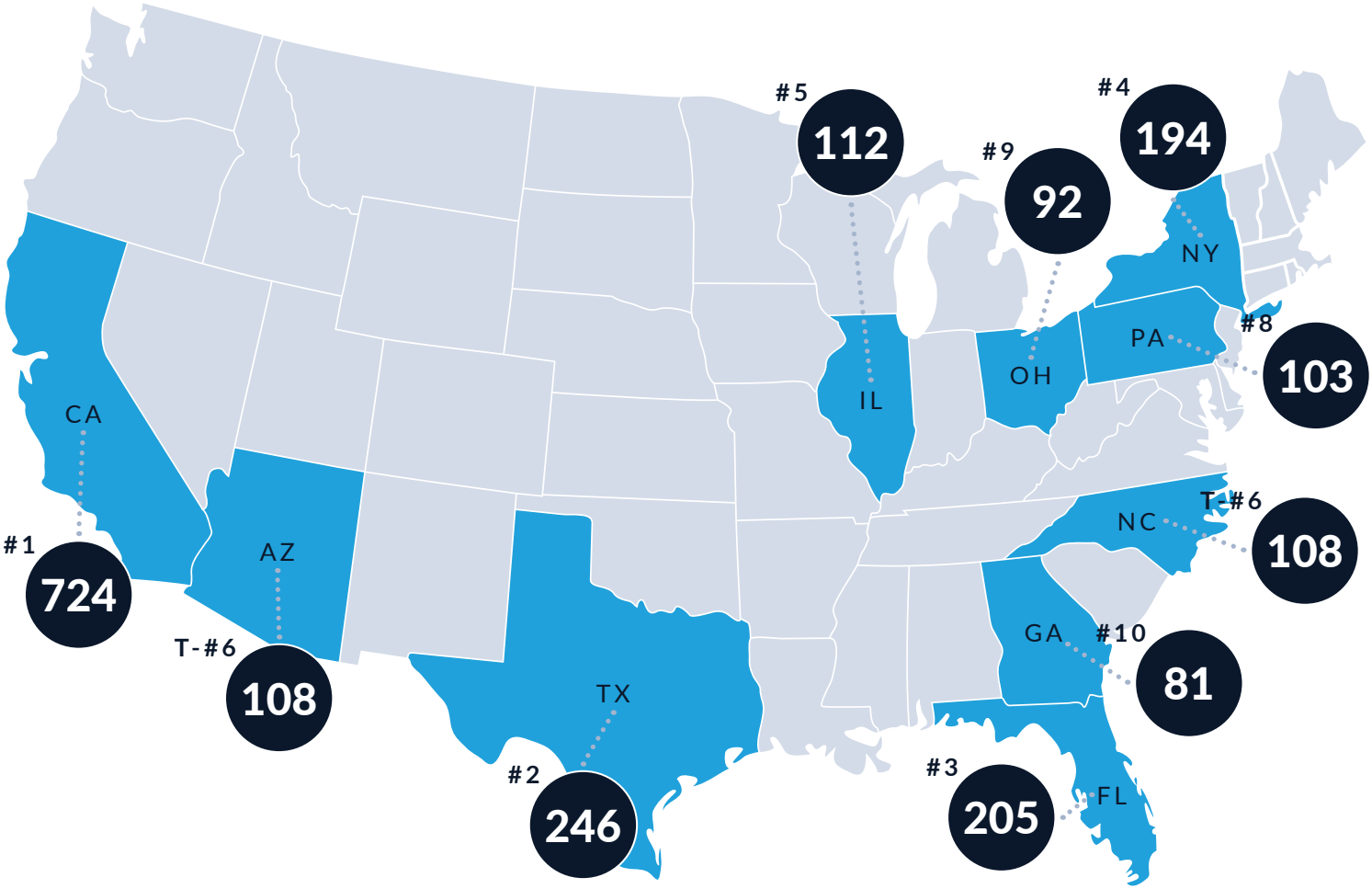
Reports of Compromise by Top 10 States

	Breach	Mail Opened	Physical Items Stolen	Picture of PII Doc Taken/ Sent/Posted	PII Found on Dark Web	Scam PII Shared	Unauthorized Access to Computer/ Mobile Device	**Total Reports of Compromise**
CA	12%	1%	33%	1%	3%	28%	17%	**11%**
TX	10%	0%	20%	0%	2%	22%	46%	**6%**
FL	3%	0%	32%	3%	3%	48%	10%	**4%**
NY	4%	0%	19%	15%	0%	52%	11%	**4%**
MA	6%	0%	13%	0%	6%	56%	13%	**2%**
NC	20%	0%	20%	0%	7%	33%	20%	**2%**
WA	7%	0%	14%	0%	7%	57%	14%	**2%**
AR	0%	0%	0%	0%	0%	100%	0%	**2%**
MN	0%	8%	8%	17%	0%	42%	25%	**2%**
AZ	9%	0%	0%	0%	0%	55%	36%	**2%**

MISUSE

By State

TOP 10 STATES BY TOTAL VICTIMS



MISUSE BY TYPE

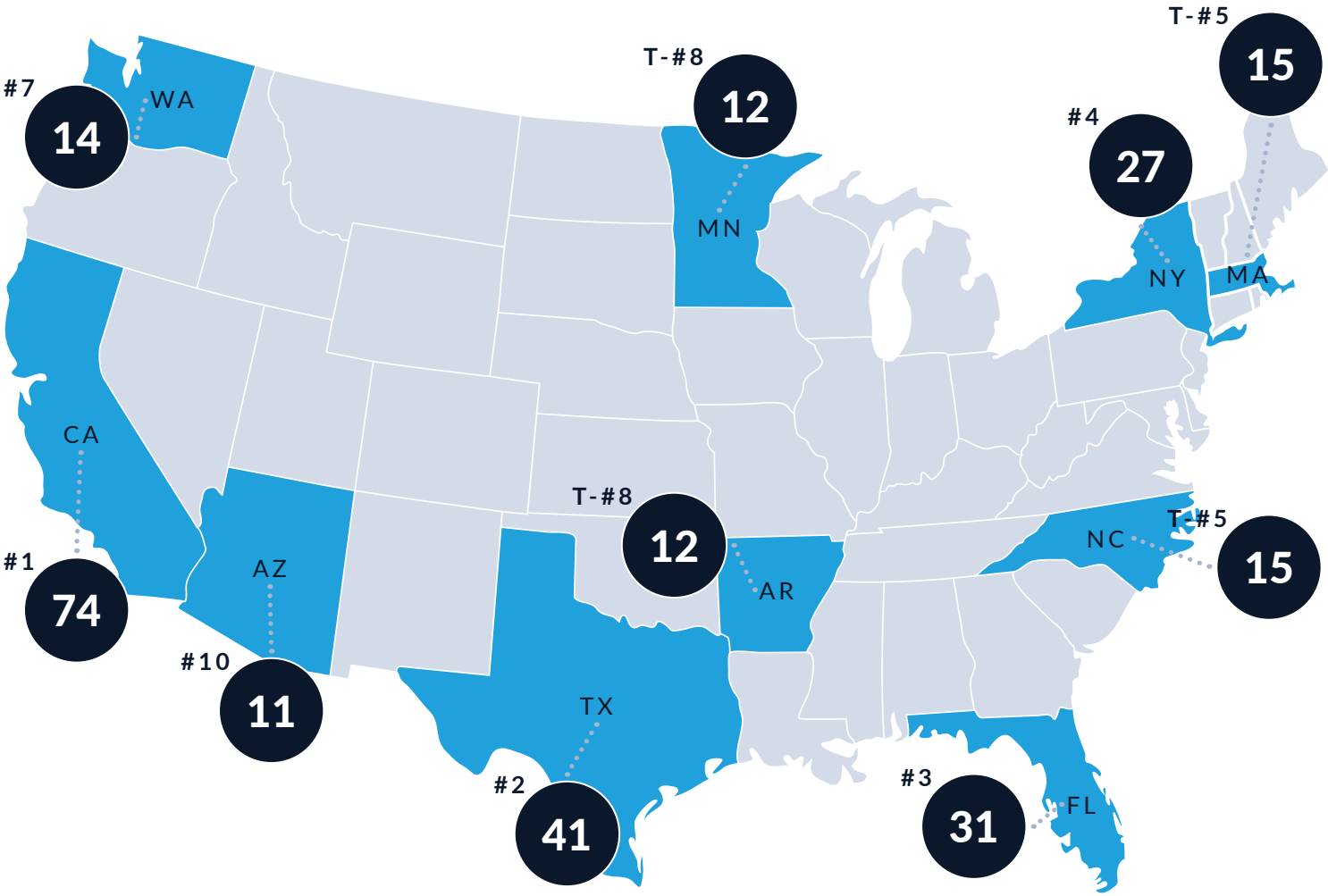
	Crime Committed Using PII	*Existing Account Takeover*	*Fraudulent Employment*	*IRS Misuse*	*New Account Created*	***Total***
Alabama	3	10	1	0	16	**30**
Alaska	0	2	0	0	2	**4**
Arkansas	2	17	1	0	10	**30**
Arizona	7	25	31	7	38	**108**
California	38	314	67	30	275	**724**
Colorado	3	21	4	0	14	**42**
Connecticut	2	11	0	0	15	**28**

	Crime Committed Using PII	Existing Account Takeover	Fraudulent Employment	IRS Misuse	New Account Created	Total
District of Columbia (D.C.)	0	6	0	0	4	10
Delaware	0	4	0	0	7	11
Florida	8	104	3	3	87	205
Georgia	6	34	5	1	35	81
Hawaii	0	2	0	0	2	4
Iowa	0	21	1	2	12	36
Idaho	0	16	2	1	6	25
Illinois	1	46	19	3	43	112
Indiana	2	23	7	0	16	48
Kansas	3	11	2	0	11	27
Kentucky	2	6	1	0	6	15
Louisianna	1	11	1	0	23	36
Massachusetts	5	37	3	0	29	74
Maryland	5	39	4	0	32	80
Maine	1	7	0	0	4	12
Michigan	3	28	0	1	15	47
Minnesota	1	29	1	1	21	53
Missouri	4	30	2	0	18	54
Mississippi	0	12	2	0	6	20
Montana	0	4	0	0	4	8
North Carolina	7	63	0	1	37	108
North Dakota	1	1	2	0	4	8
Nebraska	2	0	2	0	10	14
Nevada	1	4	1	0	19	25
New Hampshire	0	4	0	0	2	6
New Jersey	8	23	4	0	21	56
New Mexico	4	22	3	0	15	44
New York	7	112	7	8	60	194
Ohio	4	44	6	5	33	92
Oklahoma	3	9	2	0	11	25
Oregon	2	26	2	0	21	51
Pennsylvania	3	44	8	4	44	103
Rhode Island	0	0	0	0	3	3
South Carolina	3	25	2	0	22	52
South Dakota	0	3	0	0	2	5
Tennessee	4	23	0	1	18	46
Texas	9	96	19	19	103	246
Utah	0	4	1	0	8	13
Virginia	4	28	2	0	12	46
Vermont	0	1	0	0	0	1
Washington	7	20	6	1	22	56
Wisconsin	2	25	0	0	15	42
West Virginia	1	4	0	0	1	6
Wyoming	1	0	1	0	4	6
Puerto Rico	2	1	0	0	0	3
Totals	**203**	**2,464**	**262**	**41**	**1,678**	**4,648**

COMPROMISE

By State

TOP 10 STATES BY TOTAL VICTIMS



COMPROMISE BY TYPE

	Breach	*Mail Opened*	*Physical Item(s) Stolen*	*Picture of PII Taken/Sent/Posted*	*PII Found on Dark Web*	*Scam – PII Shared*	*Unauthorized Access to Device*	***Total***
Alabama	3	0	0	0	0	1	0	**4**
Alaska	0	0	0	0	0	0	0	**0**
Arkansas	0	0	0	0	0	12	0	**12**
Arizona	1	0	0	0	0	6	4	**11**
California	9	1	26	1	2	22	13	**74**
Colorado	0	0	3	0	0	1	1	**5**
Connecticut	1	0	0	0	0	1	0	**2**

	Breach	Mail Opened	Physical Item(s) Stolen	Picture of PII Taken/Sent/Posted	PII Found on Dark Web	Scam – PII Shared	Unauthorized Access to Device	**Total**
District of Columbia (D.C.)	0	0	0	0	0	0	0	**0**
Delaware	0	0	0	1	0	3	0	**4**
Florida	1	0	10	1	1	15	3	**31**
Georgia	1	0	2	0	0	5	0	**8**
Hawaii	0	0	0	0	0	1	1	**2**
Iowa	0	0	2	1	0	0	1	**4**
Idaho	0	0	1	0	0	4	0	**5**
Illinois	3	0	1	0	1	4	2	**11**
Indiana	1	0	1	0	1	4	3	**10**
Kansas	0	0	0	0	0	2	0	**2**
Kentucky	0	0	0	0	0	3	1	**4**
Louisianna	1	0	1	0	1	1	0	**4**
Massachusetts	1	0	2	0	1	9	2	**15**
Maryland	2	0	1	0	0	4	4	**11**
Maine	0	0	0	0	0	0	0	**0**
Michigan	0	0	1	0	1	3	3	**8**
Minnesota	0	1	1	2	0	5	3	**12**
Missouri	0	0	1	0	1	4	1	**7**
Mississippi	1	0	0	0	1	1	1	**4**
Montana	0	0	0	0	0	0	0	**0**
North Carolina	3	0	3	0	1	5	3	**15**
North Dakota	0	0	0	0	0	0	0	**0**
Nebraska	0	0	0	0	0	1	0	**1**
Nevada	1	0	1	0	0	6	0	**8**
New Hampshire	0	0	0	0	0	1	0	**1**
New Jersey	2	0	2	0	0	1	1	**6**
New Mexico	0	0	0	0	0	0	0	**0**
New York	1	0	5	4	0	14	3	**27**
Ohio	1	1	0	0	1	1	3	**7**
Oklahoma	1	0	0	0	1	1	0	**3**
Oregon	0	0	1	0	0	2	0	**3**
Pennsylvania	0	1	2	0	0	5	2	**10**
Rhode Island	0	0	0	0	0	1	0	**1**
South Carolina	2	0	2	0	0	1	1	**6**
South Dakota	0	0	0	0	0	0	0	**0**
Tennessee	0	0	2	0	0	5	1	**8**
Texas	4	0	8	0	1	9	19	**41**
Utah	0	0	0	0	0	2	1	**3**
Virginia	0	0	2	0	0	4	2	**8**
Vermont	0	0	0	0	0	0	0	**0**
Washington	1	0	2	0	1	8	2	**14**
Wisconsin	4	0	1	0	0	4	0	**9**
West Virginia	0	0	0	0	0	0	1	**1**
Wyoming	0	0	0	0	0	1	0	**1**
Puerto Rico	0	0	0	0	0	0	0	**0**
Totals	**88**	**4**	**118**	**15**	**28**	**317**	**141**	**711**

VICTIM DATA

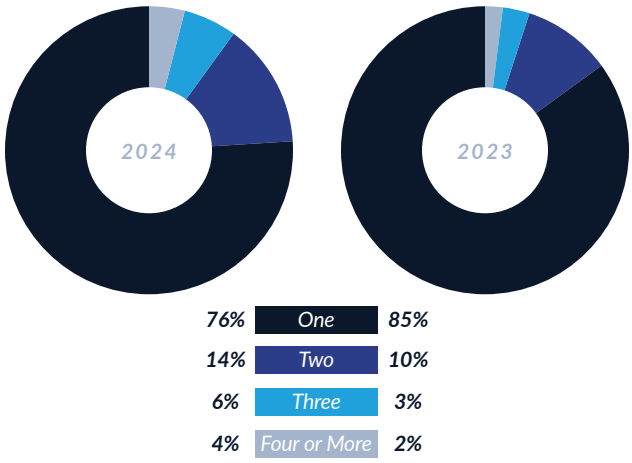
CONTACTS TO THE ITRC

From 4/1/24 – 3/31/25, 7,580 individuals contacted the ITRC with an identity-related concern, 31 percent (31%) fewer than the same period last year.

The ITRC's Advisors spoke with 6,357 individuals, 33 percent (33%) less than the same period in 2024.

More individuals who contacted the ITRC reported experiencing multiple identity-related concerns compared to contacts year-over-year.

Number of Identity Crime Instances, Year-Over-Year



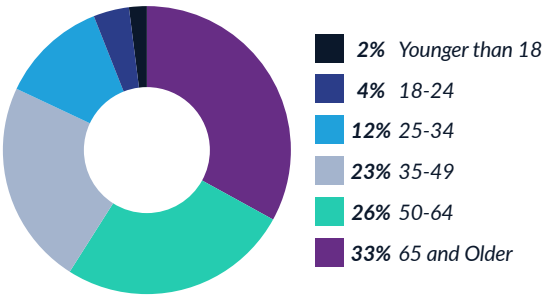
Individuals with identity-related concerns preferred to speak with someone over the phone (76%) compared to chat (17%) or email (5%). They also reach out via web form (1%), text (1%) and letter (<1%).

DEMOGRAPHIC DATA

AGE

Of the individuals willing to share their age range, individuals in older age categories reported identity-related concerns more than individuals in younger age categories.

Age



The primary concern for children was fraudulent employment using the child's personal information. Age categories 18-24, 50-64 and 65+ were mainly concerned with sharing personal information during a scam. Age categories 25-34 and 35-49 had a more evenly distributed report of concerns.

Top concerns reported for each age group:

Younger than 18

+ Fraudulent Employment (42%)
+ Data Breach (8%)
+ Fraudulent New Checking Account (4%)

18-24

+ PII Shared During a Scam (18%)
+ Stolen Documents with Personal Information (7%)
+ Social Media Account Takeover (6%)
Fraudulent New Checking Account (6%)

25-34

+ PII Shared During a Scam (9%) | Fraudulent New Credit Cards (9%)
+ Stolen Documents with Personal Information (8%)
+ Fraudulent Employment (6%)

35-49

+ Fraudulent New Credit Cards (8%)
+ PII Shared During a Scam (7%) | Stolen Documents with Personal Information (7%) Checking Account Takeover (7%)

50-64

+ PII Shared During a Scam (13%)
+ Fraudulent New Checking Account (8%)
+ Unauthorized Access to a Mobile Device (7%)

65 and Older

+ PII Shared During a Scam (23%)
+ Checking Account Takeover (9%)
+ Data Breach (7%) | Credit Card Account Takeover (7%)

ETHNICITY

Not all people who contacted the ITRC with identity concerns shared their ethnicity. However, among those who did, the breakout included:

Ethnicity

Reported Ethnicity	*Percentage*
White	53%
Hispanic or Latino or Spanish Origin of Any Race	19%
Black or African American	18%
Two or More Races	5%
Asian	5%
American Indian or Alaskan Native	1%
Native Hawaiian or Other Pacific Islander	0.2%

Top concerns reported by each ethnic group:

Hispanic or Latino or Spanish Origin of Any Race

+ Fraudulent Employment (12%)
+ PII Shared During a Scam (10%)
+ Fraudulent New Credit Card (9%)

American Indian or Alaskan Native

+ Stolen Documents with Personal Information (11%)
+ Unauthorized Access to a Mobile Device (11%)

Asian

+ PII Shared During a Scam (17%)
+ Checking Account Takeover (9%)
+ Stolen Documents with Personal Information (8%)

Native Hawaiian or Other Pacific Islander

+ Fraudulent Employment (43%)
+ PII Shared During a Scam (14%)
+ Stolen Documents with Personal Information (14%)

Black or African American

+ PII Shared During a Scam (9%)
+ Stolen Documents with Personal Information (7%)
+ Checking Account Takeover (6%)

White

+ PII Shared During a Scam (17%)
+ Fraudulent New Credit Card (8%)
+ Checking Account Takeover (6%) | Credit Card Account Takeover (6%) | Unauthorized Access to a Mobile Device (6%)

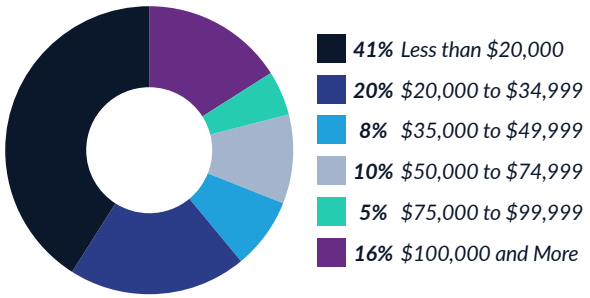
Two or More Races

+ Checking Account Takeover (11%)
+ Fraudulent Employment (7%)
+ PII Shared During a Scam (6%) | Stolen Documents with Personal Information (6%)

INCOME

Of the individuals willing to share their income range, reports of identity-related concerns were primarily reported by individuals in the lower income ranges.

Income



In all income ranges except the lowest, the primary concern was sharing personal information during a scam. Individuals who reported making less than $20,000 reported a myriad of concerns.

Top concerns reported by each income level:

Less than $20,000

+ Fraudulent New Credit Card (8%) | Stolen Documents with Personal Information (8%) PII Shared During a Scam (8%) | Unauthorized Access to a Mobile Device (8%)

$20,000 to $34,999

+ PII Shared During a Scam (15%)
+ Fraudulent New Credit Card (7%) | Stolen Documents with Personal Information (7%)
+ Checking Account Takeover (6%) | Fraudulent Employment (6%)

$35,000 to $49,999

+ PII Shared During a Scam (21%)
+ Checking Account Takeover (9%)
+ Fraudulent New Credit Card (7%)

$50,000 to $74,999

+ PII Shared During a Scam (19%)
+ Checking Account Takeover (7%) | Fraudulent New Credit Card (7%)
+ Unauthorized Access to a Mobile Device (6%)

$75,000 to $99,999

+ PII Shared During a Scam (23%)
+ Fraudulent New Credit Card (9%)
+ Checking Account Takeover (7%)

$100,000 and More

+ PII Shared During a Scam (16%)
+ Credit Card Account Takeover (11%)
+ Fraudulent New Credit Card (9%)

GENDER

Of the individuals willing to share their gender, reports of identity-related concerns were primarily reported by females.

Gender

Top concerns reported by each gender:

Males

+ PII Shared During a Scam (16%)
+ Fraudulent New Credit Card (8%)
+ Checking Account Takeover (6%)

Females

+ PII Shared During a Scam (14%)
+ Checking Account Takeover (7%) | Fraudulent New Credit Card (7%)
+ Stolen Documents with Personal Information (6%) | Unauthorized Access to a Mobile Device (6%)

SPECIFIC POPULATIONS

Of the individuals who self-identified as part of a specific population, reports of identity-related concerns were primarily reported as follows:

Specific Populations

Reported Specific Population	Percentage
Blind/Vision Impaired	7%
Deaf/Hearing Impaired	3%
Domestic Violence Survivor	24%
Former/Foster Youth	4%
Homeless	18%
Incarcerated	3%
Formerly Incarcerated	13%
Active-Duty Military	1%
Military Veteran	15%
Student	1%
Trafficking Survivor	11%

Top concerns reported by each population:

Blind/Vision Impaired

+ PII Shared During a Scam (16%)
+ Checking Account Takeover (13%)
+ Unauthorized Access to a Mobile Device (10%)

Deaf/Hearing Impaired

+ PII Shared During a Scam (27%)
+ Checking Account Takeover (13%) | Data Breach (13%)

Domestic Violence Survivor

+ Fraudulent New Credit Card (16%)
+ Unauthorized Access to a Mobile Device (9%)
+ Stolen Documents with Personal Information (8%)

Former/Foster Youth

+ Data Breach (11%) | IRS Misuse (11%) Checking Account Takeover (11%)

Homeless

+ Fraudulent New Credit Card (12%) | Stolen Documents with Personal Information (12%)
+ Checking Account Takeover (7%) Unauthorized Access to a Mobile Device (7%)

Incarcerated

+ Checking Account Takeover (17%) | Fraudulent New Credit Card (17%) | Stolen Documents with Personal Information (17%)

Formerly Incarcerated

+ Fraudulent New Credit Card (11%)
+ Checking Account Takeover (10%)
+ IRS Misuse (8%)

Active-Duty Military

+ Fraudulent New Credit Card (25%) Fraudulent New Checking Account (25%) PII Shared During a Scam (25%)

Military Veteran

+ Checking Account Takeover (16%)
+ Fraudulent New Credit Card (9%) Stolen Documents with Personal Information (6%)

Student

+ PII Shared During a Scam (33%)
+ Credit Card Account Takeover (17%)
+ Data Breach (17%)

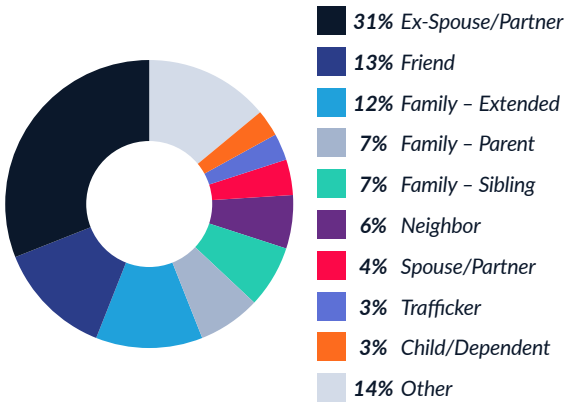
Trafficking Survivor

+ Fraudulent New Credit Card (18%)
+ Fraudulent New Checking Account (8%)
+ Credit Card Account Takeover (6%) Fraudulent New Auto Loan (6%) Unauthorized Access to a Mobile Device (6%)

VICTIM VS. THIEF

A majority of individuals (88%) did not know the identity of the thief. Of those who did, a large percentage of victims alleged it was their ex-spouse/partner.

Alleged Thief

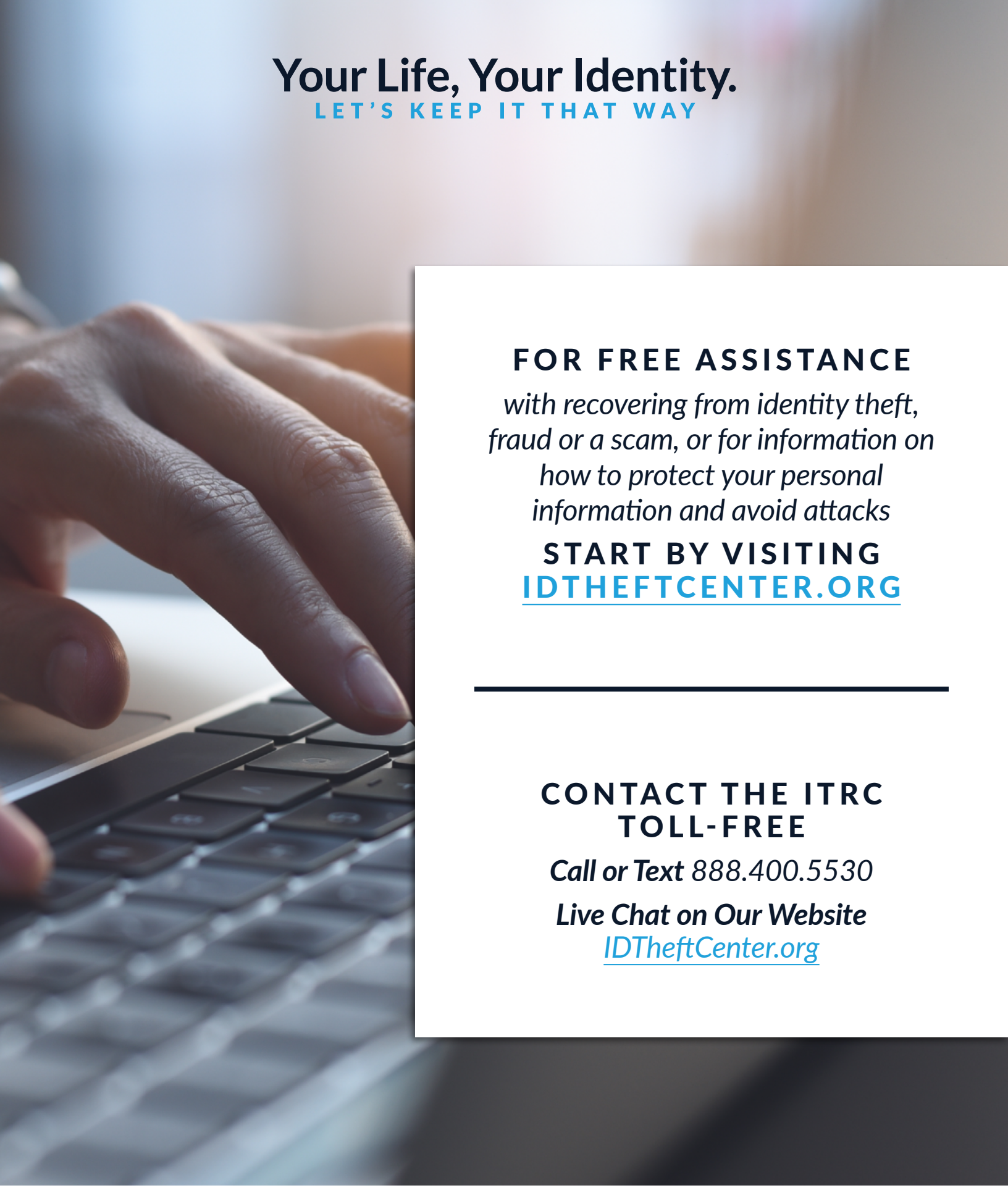


Most individuals reported their own identity concerns (90%). Of those reporting identity concerns on behalf of someone else, they primarily reported that the victim was a child/dependent.

Victim Being Reported

	Percentage
Child/Dependent	34%
Spouse/Partner	19%
Child/Dependent – Adult	8%
Family – Parent	7%
Deceased	5%
Friend	4%
Deceased; Spouse/Partner	4%
Family – Sibling	3%

	Percentage
Family – Extended	3%
Deceased; Family – Parent	3%
Business/Non-Profit	3%
Deceased; Family – Extended	1%
Deceased; Family – Sibling	1%
Business/Non-Profit; Self	1%
Client – Advocate	1%
Other	3%



Your Life, Your Identity.

LET'S KEEP IT THAT WAY

FOR FREE ASSISTANCE

with recovering from identity theft, fraud or a scam, or for information on how to protect your personal information and avoid attacks

START BY VISITING
IDTHEFTCENTER.ORG

CONTACT THE ITRC TOLL-FREE

Call or Text *888.400.5530*

Live Chat on Our Website
IDTheftCenter.org

ITRC | IDENTITY THEFT RESOURCE CENTER