MAY 2023

ITRC | IDENTITY THEFT RESOURCE CENTER

2022 TRENDS IN IDENTITY REPORT

idtheftcenter.org • 1-888-400-5530

IDENTITYIQ by IDIQ

*This report was made possible through the support of **IdentityIQ**.*

Table of Contents

CEO Letter

In the year since the Identity Theft Resource Center published our first Trends in Identity report, the identity crime landscape has changed.

In the year since the Identity Theft Resource Center published our first Trends in Identity report, the identity crime landscape has changed. Some of the changes have been dramatic, like the shift away from transparency in data breach notices. Other issues have been unexpected, like the research findings showing Black communities suffer significantly larger financial losses than the general population from identity crimes.

But, one thing has not changed: There are too many victims of identity compromise and misuse and too few resources to help them.

For more than two decades, the ITRC did not publish findings gleaned from the identity crime victims and concerned consumers who contact us each day. As the complexity and sheer volume of identity crimes grew over time, so did our belief that we needed to share the trends we saw in their earliest stages.

Last year we highlighted the dramatic growth in social media account takeover. What started as a handful of reports of being locked out of Facebook or Instagram accounts in 2021 quickly grew into a trend that ITRC research determined in 2022 had far-reaching financial impacts on individuals and small businesses.

In the pages that follow, we're going to explore key findings based on contacts from nearly 15,000 reports to the ITRC of identity compromises, misuse, or abuse from individuals across the country. We're specifically going to focus on three trends. Identity criminals are:

Getting better at convincing people to share personal information through social engineering. In the *2021 Trends in Identity Report*, we noticed identity thieves were exploiting social media to offer money-earning opportunities. In 2022, thieves started to shift their tactics.

Misusing information stolen through data compromises more often. Most concerning is the increase in reports of Social Security numbers being misused to gain employment and misused by individuals committing crimes.

Targeting Driver's License accounts to help commit identity fraud. A fake driver's license isn't just for underage college kids anymore. Victims contacting the ITRC share how identity thieves misused their stolen driver's license information to obtain auto loans, open new bank accounts, and open cell phone accounts, among other criminal actions.

All of these trends arrive at a time when there is growing concern at all levels of government and in the private sector about the overwhelming number of identity crimes and the toll of identity fraud on individuals and businesses. Earlier this year, the Biden Administration published a national cyber strategy that included key provisions designed to address identity fraud and the lack of support for identity crime victims.

The presidential planning document points to the need for government agencies and nonprofits like the ITRC to work together to ease the burden on victims who often do not know where to turn for help or how to begin to recover their identities. We look forward to working with our nation's leaders to bring the vision of improved services for identity crime victims to reality.

A special word of thanks to IDIQ and their support of the *2022 Trends in Identity Report*. We appreciate them and all of our supporters who help ensure we continue to offer free assistance to individuals who are victims of identity crimes – and reports like this and our other analysis and research materials for business and government leaders.

I hope you will find the information in this *Trends in Identity Report* both valuable and thought-provoking. You can always reach out to us for more information via online chat, email, or phone call.

Thank you for your interest in our report and the ITRC.

Eva Velasquez, *CEO*

Identity Theft Resource Center
May 2023

2022 TRENDS IN IDENTITY REPORT

idtheftcenter.org • 1-888-400-5530

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

IDENTITYIQ by IDIQ *This report was made possible through the support of IdentityIQ.*

2022 Reported Identity Crimes

14,817
TOTAL CRIMES REPORTED

Less Than
1% Decrease
FROM 2021

COMPROMISED CREDENTIALS
55% – 8,199 CASES

MISUSED CREDENTIALS
40% – 5,961 CASES

REQUESTING PREVENTION
3% – 437 CASES

ATTEMPTED MISUSE
1% – 220 CASES

2022 Identity Misuse

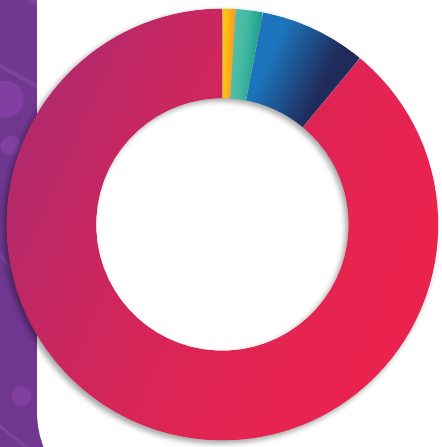
61%
EXISTING ACCOUNT TAKEOVER (ATO)

32%
NEW ACCOUNT CREATION

IDENTITY MISUSE BY CATEGORY

Existing Account Takeover		*New Account Creation*
88%	NON-GOVERNMENT, NON-FINANCIAL	12%
48%	FINANCIAL	52%
62%	FEDERAL	38%
30%	STATE	70%

Number of Crimes Reported Per Victim in 2022



- **89%** *One Incident or Requesting Prevention*
- **8%** *Two Incidences*
- **2%** *Three Incidences*
- **1%** *Four or More Incidences*

2022 Identity Compromises

80%
COMPROMISES DUE TO A SCAM

3% Increase
FROM 2021

GOOGLE VOICE
61% – 4,081 VICTIMS

2022 Trends in Identity

+ ***Trends in Identity***
  - *2022 Discussion*
+ ***Types of Cases***
+ ***Identity Misuse***
  - *Existing Account Takeover*
  - *New Account Creation*
  - *Attempted Misuse*
+ ***Identity Compromises***

Trends in Identity

The core of the ITRC since 1999 has been the Contact Center and its expert advisers. This report is based on conversations with victims whose personal information was compromised or misused in an identity crime. The trends discussed here also include contacts from people who want to avoid becoming an identity crime victim.

While the discussion that follows is based on 2022 statistics, it's worth noting that the early trends from 2023 point to significant changes ahead this year. Specifically, in Q1 2023:

The number of overall contacts grew in Q1 2023 compared to the same period in 2022.

The number of victims who contacted the ITRC for assistance regarding multiple accounts being compromised grew, while the number of people reporting single accounts being compromised dropped by ten percentage points.

More victims contacted the ITRC due to the compromise of personal information than misuse by nearly 20 percentage points.

There has been a surge in the number of people requesting preventative information.

2022 Discussion

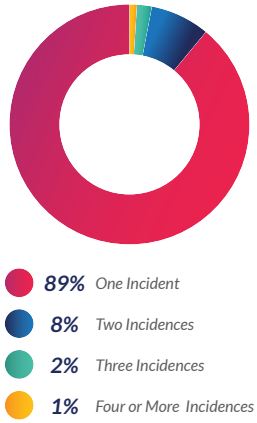
In 2022, the ITRC had a similar number of reported identity crimes (compromise, theft, and misuse) to its all-time high in 2021: 14,817 in 2022 compared to 14,947 in 2021, a decrease of less than one percent (1%).

Beginning in 2022, the ITRC tracked the number of identity crimes reported per victim. The ITRC assisted 12,911 victims with a new identity concern. Of those victims:

- Eighty-nine percent (89%) reported experiencing a single incidence of an identity crime or just wanted to request preventative information.
- Eight percent (8%) reported being a victim of two (2) incidences of an identity crime.
- Two percent (2%) reported being a victim of three (3) incidences of an identity crime.
- One percent (1%) reported being a victim of four (4) or more identity crimes.

See Figure 1

Figure 1 | *Number of Incidences Reported by a Victim*



ITRC Advisors open three types of cases when contacted by a victim: identity misuse (actual and attempted), identity compromise, or prevention.

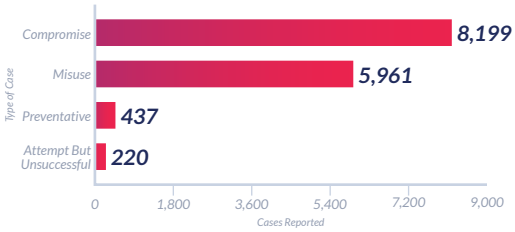
Misuse is when there is evidence that a person's identity information has been or is actively being misused by an identity criminal. The ITRC also tracks attempts to misuse identity information. Compromise means personal information has been exposed and is at risk of being misused, but no abuse is known to have occurred. Prevention is a request for information.

In 2022, 55 percent (55%) of identity crime cases reported were due to compromised credentials. Forty percent (40%) of reported cases were due to misuse of credentials. One percent (1%) of reported identity crime cases were due to victims being notified about attempted but unsuccessful misuse of their credentials. Three percent (3%) of cases were people requesting preventative information due to a concern about their identity, but no reported compromise, theft, or misuse.

See Figure 2

This represents a significant shift from the prior two (2) years when more than 70 percent (70%) of identity crimes reported to the ITRC were regarding compromise, attempted misuse, or requesting preventative information, and more than 26 percent (26%) of identity crimes were due to actual misuse of credentials.

Figure 2 | *Identity Crime Cases Reported*



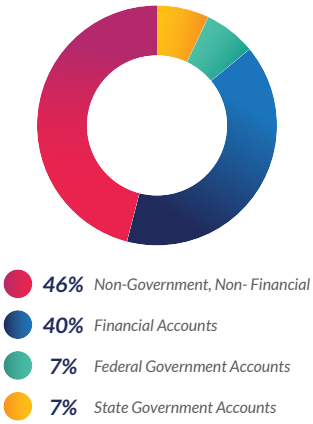
Identity misuse, in general, was primarily due to account takeover or new account creation in 2022.

Forty-six percent (46%) of non-governmental and non-financial accounts were misused. Forty percent (40%) of financial accounts were misused, of which 44 percent (44%) involved credit card accounts and 33 percent (33%) bank accounts. Seven percent (7%) of federal accounts were misused – 78 percent (78%) due to IRS accounts – and seven percent (7%) of state accounts – 71 percent (71)% due to unemployment accounts.

See Figure 3

- Misused social media accounts made up seventy-two percent (72%) or non-government, non-financial account abuse.
- DMV accounts made up four percent (4%) of misused government accounts (state and federal) in 2021, but increased to fifteen percent (15%) in 2022.
- In 2022, four percent (4%) of misuse victims discovered a crime was committed using their personal information, up from three percent (3%) in 2020 and 2021.
- Two percent (2%) of misuse victims discovered someone was working using their Social Security number in 2022 – this is up from 2020 (0.5%) and 2021 (0.2%).
- One percent (1%) of misuse victims discovered an account in collections or had another type of misuse.

Figure 3 | *Account Type Involved in Identity Misuse*



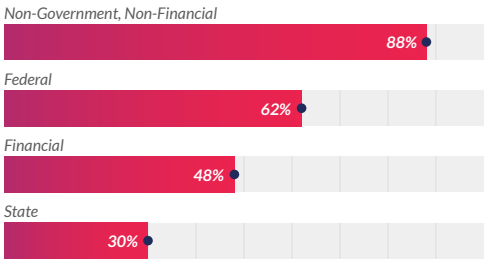
Existing Account Takeover (ATO)

The majority of reported identity misuse was due to existing account takeover (61% – 3,637 victims).

In 2022, 88 percent (88%) of non-government, non-financial accounts, 62 percent (62%) of federal accounts, 48 percent (48%) of financial accounts, and 30 percent (30%) of state accounts were impacted by existing account takeover.

See Figure 4

Figure 4 | *Sectors of Existing Account Takeover*

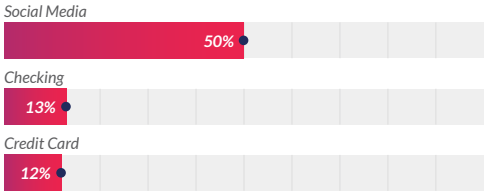


By Category

- IRS accounts were the federal account type most often impacted by ATO at 84 percent (84%).
- Checking accounts were the financial account type most often impacted at 46 percent (46%), followed closely by credit card accounts at 41 percent (41%).
- Social media accounts were the non-government, non-financial account type most often impacted by existing account takeover at 81 percent (81%).
- Unemployment accounts were the state account type most impacted at 57 percent (57%); DMV accounts were the next highest at 25 percent (25%).

See Figure 5

Figure 5 | *Top Three ATO by Account*



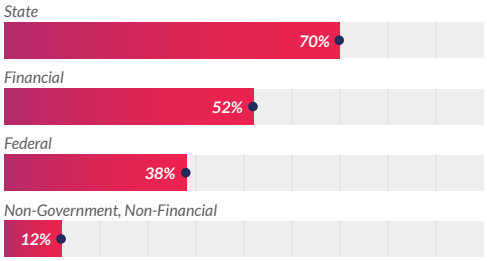
New Account Creation

Second to existing account takeover in 2022 was misuse related to new account creation (32% – 1,889 victims).

This type of misuse impacted 70 percent (70%) of state accounts, 52 percent (52%) of financial accounts, 38 percent (38%) of federal accounts, and 12 percent (12%) of non-government, non-financial accounts.

See Figure 6

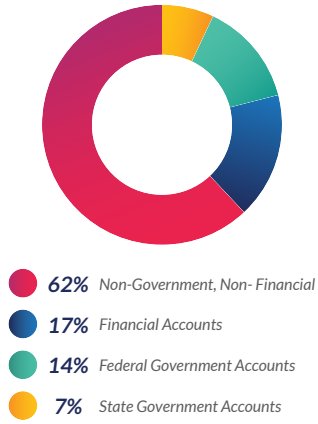
Figure 6 | *Sectors of New Account Creation*



Of all new accounts created by identity criminals in 2022, 62 percent (62%) were financial accounts, 17 percent (17%) were non-government, non-financial accounts, 14 percent (14%) were state accounts, and seven percent (7%) were federal accounts.

See Figure 7

Figure 7 | *New Account Creation by Account Type*

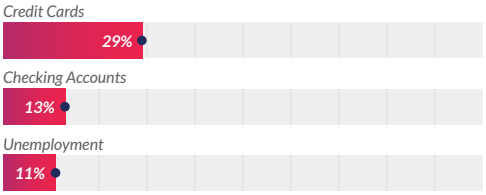


By Category

- IRS accounts were the federal account type most often impacted by new account creation at 68 percent (68%) related to taxes filed on behalf of children and/or non-filers.
- Credit card accounts were the financial account type most often impacted at 47 percent (47%). Bank accounts were the next highest at 20 percent (20%).
- Undisclosed accounts were the most reported non-government, non-financial account type most often impacted by new account creation at 22 percent (22%), followed by cell phone accounts 18 percent (18%).
- Unemployment accounts were the state account type most impacted at 78 percent (78%); DMV accounts were the next highest at ten percent (10%).

See Figure 8

Figure 8 | *Top Three New Accounts Created by Account*



Attempted Misuse

This is a new category based on reports from victims who had been informed of attempted fraudulent activity on an existing account or an unsuccessful attempt to create a new account in the victim's name. Victims who contacted the ITRC were concerned about the risk to their identity and wanted advice on how to protect their personal information from further attack.

Of the unsuccessful attempts to misuse identity information, financial accounts were most targeted – 80 percent (80%) of reported attempts involved an existing account, and 85 percent (85%) involved a new account.

See Figure 9

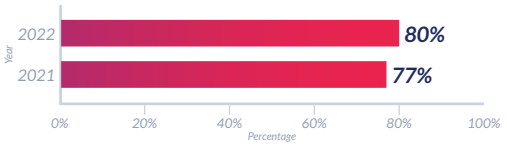
Figure 9 | *Attempted Misuse of Financial Accounts*

Identity Compromises

In 2022, 80 percent (80%) of identity compromises involved the use of identity credentials as part of a scam, compared to 77 percent (77%) in the previous year.

See Figure 10

Figure 10 | *Identity Credentials Compromised as Part of a Scam*



An overwhelming majority of people who contacted the ITRC about compromised identities in 2022 were victims of a Google Voice scam (61% – 4,081 victims). In 2021, Google Voice was also the top reported scam (53% – 3,926 victims). Seven percent (7%) of victims reported government grant scams (531 victims), closely followed by phony government agency representations (7% – 519 victims).

The remaining victim contacts generally involved some form of impersonation designed to get a victim to reveal personal information or credentials:

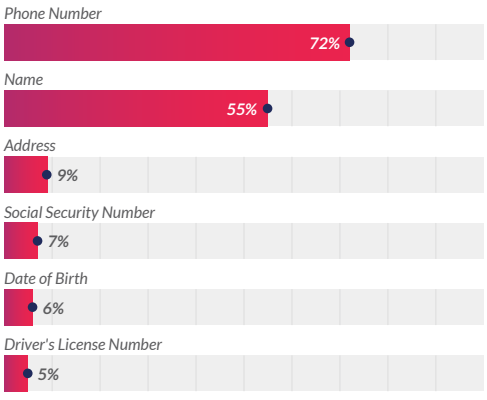
- Seven percent (7% – 438 victims) were contacted by a criminal pretending to be a legitimate business or organization (CVS, PayPal, cable company, etc.)
- Six percent (6% – 370 victims) were contacted by a criminal pretending to represent a government agency (Department of Homeland Security, IRS, etc.)
- Four percent (4% – 297 victims) were contacted by a person claiming to represent a lottery or organization offering a prize (Publisher's Clearinghouse, etc.)

Scam victims reported the following personal information was exposed alone or in combination with other personal information:

- ***Phone Number*** – 72%
- ***Name*** – 55%
- ***Address*** – 9%
- ***Social Security Number*** *(Full/Partial)* – 9%
- ***Date of Birth*** – 6%
- ***Driver's License Number*** – 5%

See Figure 11

Figure 11 | *Personal Information Exposed Due to a Scam*

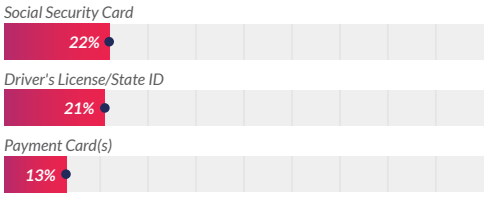


Nine percent (9%) of reported compromises were due to physical items were due to items being stolen or lost.

- ***Stolen Items*** – 85%
- ***Lost Items*** – 15%

See Figure 12

Figure 12 | *Top Three Most Reported Items Lost/Stolen*



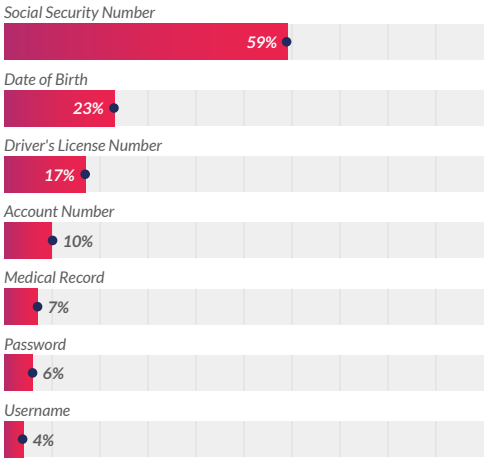
Five percent (5%) of reported compromises were due to unathorized access to a computer or mobile device.

Three percent (3%) of reported compromises in 2022 were due to a data breach, compared to one percent (1%) in 2021. Data breach victims reported the exposure of various forms for personal information, alone or in combination with other PII:

- ***Social Security Number*** *(Full/Partial)* – 59%
- ***Date of Birth*** – 23%
- ***Driver's License Number*** – 17%
- ***Account Number*** – 10%
- ***Medical Record*** – 7%
- ***Password*** – 6%
- ***Username*** – 4%

See Figure 13

Figure 13 | *Personal Information Exposed Due to a Data Breach*



Two percent (2%) of reported compromises were due to a photo of the victim's personal information being taken, sent to someone, or posted on social media.

The remaining one percent (1%) of compromises were due to personal information being found on the dark web, someone impersonating the victim, the victim's mail being opened, or another form of compromise.

2022 Notable Trends

+ *Social Engineering*
+ *Misusing Data*
+ *Driver's License Account Targeting*

Social Engineering

Identity thieves are getting better at using social engineering techniques to convince people to share personal and business information.

In the *2021 Trends in Identity Report*, the ITRC noticed identity thieves were exploiting social media to offer opportunities to earn money. These attacks took various forms such as Google Voice scams where the threat actors pretended to be a customer. Criminals also offered opportunities to apply for a fake government grant or offered phony bitcoin investment opportunities.

In 2022, the Google Voice scam was still the top scam reported to the ITRC.

Social media takeover was still the top type of account takeover in 2022.

However, identity thieves shifted their tactics during the course of the year. Attackers found success in pretending to be a new or existing relationship to takeover a victim's friends' social media account.

The criminals would then ask victims to click on a malicious link, sometimes in a bogus "vote for me" campaign or to ask for help regaining access to a friend's account. By clicking on the link, the victim would give the impersonator access to their social media account or sensitive personally identifiable information.

The criminals on occasion also pretended to be the victims' boss or coworker to get access to business' systems, or pretended to be a company where the victim had a business relationship (and in some instances already expected to hear from) to get them to pay bogus additional charges and/or share sensitive personally identifiable information.

From the ITRC Advisor's Notes

- Victim received a call today from someone pretending to be from their cable/internet provider. The caller had the victim's Date of Birth (DOB), Name, and Address. Victim then shared their Social Security Number (SSN) with the caller.
- Victim was contacted by phone by someone pretending to be from the victim's employer, asking the victim to transfer money from their account. The victim shared their Driver's License (DL) number as well.
- Victim received a text from what they thought was their bank. They called the number in the text message resulting in an automated response. The automated system asked for the victim's DOB, SSN, credit card Info, expiration and CVV, and full name.
- Victim was expecting a technician from a cable and internet provider to visit their home. The victim received a phone call the morning of the scheduled visit from a number in a state where they previously lived. The caller claimed to be from the service provider and asked for the victim's DOB and SSN to confirm the appointment. The victim realized they had been scammed when they received a call from the real service provider in the state where the victim now lives.

Misusing Data

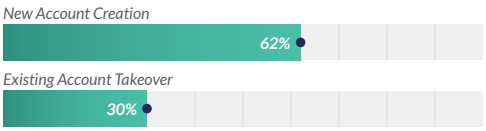
Thieves aren't just collecting information through data compromises; they're increasingly misusing data in new ways.

For at least the past five years, nearly three-quarters (75%) of victims contacting the ITRC have requested assistance after their personally identifiable information (PII) was compromised and at an increased risk of being misused[1]. Reports of misuse of both new and existing accounts were up 13 percent (13%) in 2022 compared to 2021.

While social media accounts were the primary type of account compromised in the past year, about 30 percent (30%) of existing account takeover and 62 percent (62%) of new account creation were reported as impacting financial accounts, primarily bank and credit card accounts. Other at-risk account compromises prompting victims to contact the ITRC include attempted takeover of peer-to-peer payment platforms as a vehicle for payment scams.

See Figure 14

Figure 14 | *Compromised Accounts Impacting Financial Accounts*



Federal and state benefits were also targeted by identity thieves in 2022, even though enhanced pandemic benefits expired. Most concerning was the increase in reports of Social Security numbers being misused to gain employment and misused by individuals committing crimes.

Though still somewhat time-consuming, identity misuse involving financial institutions tends to be resolved more quickly. Identity misuse involving government benefits, false employment, and criminal acts has a much longer resolution time frame with a more significant impact on daily life.

From the ITRC Advisor's Notes

+ Victim applied for food stamps and found out that someone was working under their Social Security Number.

[1]*Approximately 25 percent (25%) of victims who contact the ITRC actually had their identity credentials misused.*

- In December 2021, the victim was notified by Equifax, by email, that their email address had been changed to the thief's email address. The thief tried to lift a credit freeze. The victim also found out that their 2022 taxes were rejected, and there is an unpaid balance due to the IRS. They also found unpaid medical bills with healthcare providers and that the thief had added dependents. The thief had a green card in the victim's name.
- Victim stated they had been a victim of identity theft. Someone attempted to claim unemployment benefits under their name; the claim was denied. Victim stated that a fraudulent credit card and loan were opened in their name. Victim also said there was a homeowner's refund applied for fraudulently. Victim was notified by their mailman who noticed that their mail was being mailed to an old address.
- Victim stated someone obtained their SSN, then created and registered an LLC in New York state. The thief then went to a bank to open an account under the victim's name using a different address.
- Victim stated that someone applied for Social Security insurance benefits with their two-month-old daughter's SSN.
- Victim discovered a mortgage loan, car loan and credit cards in their name while checking their credit reports.
- Victim stated their credit card company notified them that someone had opened a mortgage loan and auto loan in the victim's name – victim has no car or mortgage.
- Victim received checks from a bank where they did not have an account. The victim went to the bank branch in their area and learned a credit card and debit card were also issued. The bank advised that the account was opened online and that the victim's Social Security Number was used. The bank closed all accounts and referred victim to ITRC.
- Victim's spouse received mail from a bank related to a new business checking account. Money was deposited into the account which was frozen but not closed. The spouse also received a letter from a different bank also relating to a new business account application that was denied due to lack of information. The fraudulent business had applied for a business license in Minnesota and then transferred the business address to Florida and also changed the home mailing address to Florida.

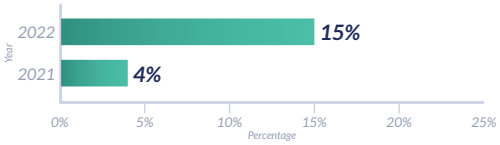
Driver's License Account Targeting

Identity criminals are targeting driver's license accounts.

In 2021, DMV accounts made up four percent (4%) of government accounts that were misused or taken over. In 2022, that number was 15 percent (15%).

See Figure 15

Figure 15 | *Misused or Taken Over DMV Accounts*



Though the volume of driver's license accounts being misused was not as high as unemployment benefit accounts, there was a significant increase year-over-year in 2022. Often, victims whose driver's license accounts were compromised discovered the misuse when they went to renew their license – but criminals had already renewed the license or there were traffic tickets attributed to the license that were not related to the victim.

Other victims went to apply for a new driver's license and could not because a thief applied for a license using the victim's information, sometimes in another state. There were also reports of fake driver's licenses being successfully used with law enforcement to evade responsibility for violations.

In 2021, the ITRC saw a rise in employment scams asking for victims to provide a copy or picture of their driver's license, primarily to use as identity verification to open other accounts. In 2022, victims stated identity thieves misused their driver's license to obtain auto loans, open new bank accounts, and open cell phone accounts.

From the ITRC Advisor's Notes

- Victim had their license stolen and replaced with a new license number. The victim has since learned that someone used the stolen license with the old number to buy a car.
- Victim has past due tickets dating back to 2020 for a car that is not theirs.

- Victim stated their employer suffered a breach where their DL and SSN were exposed. They later discovered someone opened a financial account and credit card with the stolen information. The identity thief also took all of the funds in the victim's 401k plan.
- Victim stated their mailing address was changed with the DMV. A copy of their license was used to apply for a loan to purchase a motorcycle for $29,000. The victim visited the dealership and was told the purchase was made during covid when masks were required.
- Victim stated that she completed a background check for work and was informed an MVR record was found under their name even though the victim doesn't drive or have a license yet.
- Victim learned an identity thief used the victim's ID and SSN to schedule a mail hold for two weeks with the USPS by completing a card stating the victim was on vacation. The victim also learned:
    - The thief applied for an ID in the victim's name using their SSN.
    - The thief went to the victim's bank and withdrew $21K from the victim's checking and savings accounts. The bank manager shared that the thief wore a mask and a baseball hat and, when asked to prove their identity, pulled down the mask very quickly.
    - The victim learned that multiple new credit cards, store cards, and checking accounts were opened in their name as well mobile phone accounts at two telecommunication carriers.

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).

About the ITRC & IDIQ

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.

About IDIQ®

IDIQ® is recognized as one of the fastest-growing industry leaders in identity theft protection and credit report monitoring. With the flagship IdentityIQ® and MyScoreIQ® brands, the company delivers credit report information, education and protection that benefits consumers and businesses. The company features 100% U.S.-based customer service and support. For more information, visit IDIQ.com.

2022 TRENDS IN IDENTITY REPORT

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT RESOURCE CENTER

IDENTITYIQ by IDIQ

*This report was made possible through the support of **IdentityIQ**.*

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, ***click here***.

For Media

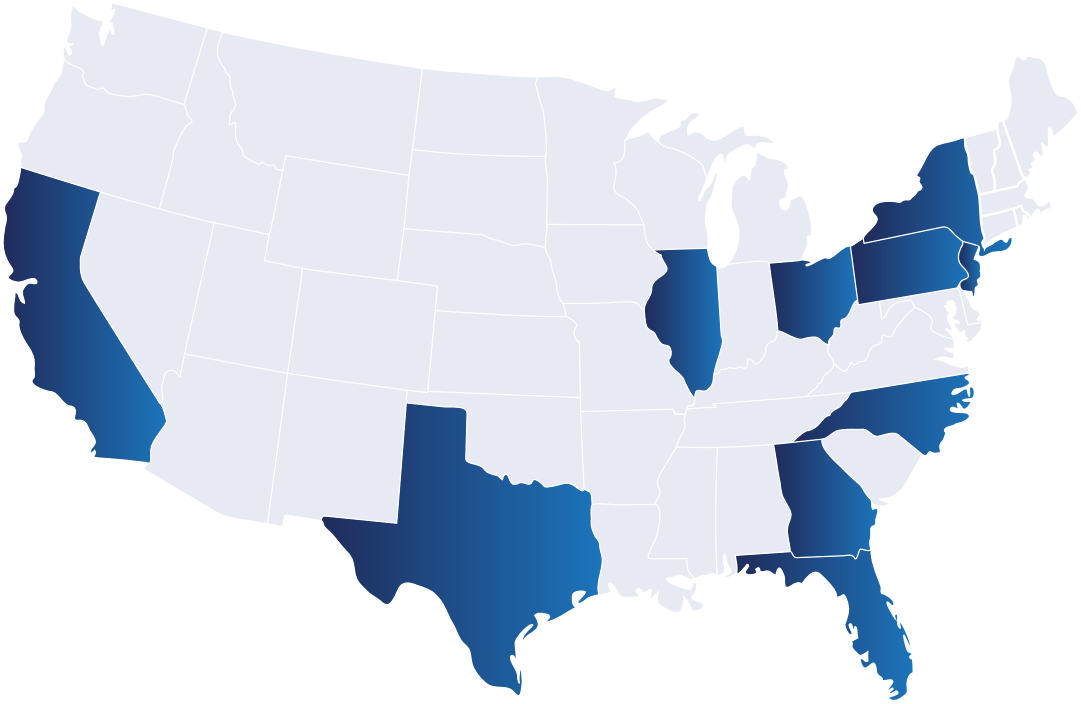
For any media-related inquiries, please email ***media@idtheftcenter.org***.

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*	***825***
2.	*Texas*	***414***
3.	*New York*	***368***
4.	*Florida*	***343***
5.	*Pennsylvania*	***215***
6.	*Illinois*	***198***
7.	*Georgia*	***159***
8.	*North Carolina*	***143***
9.	*Ohio*	***136***
10.	*New Jersey*	***130***

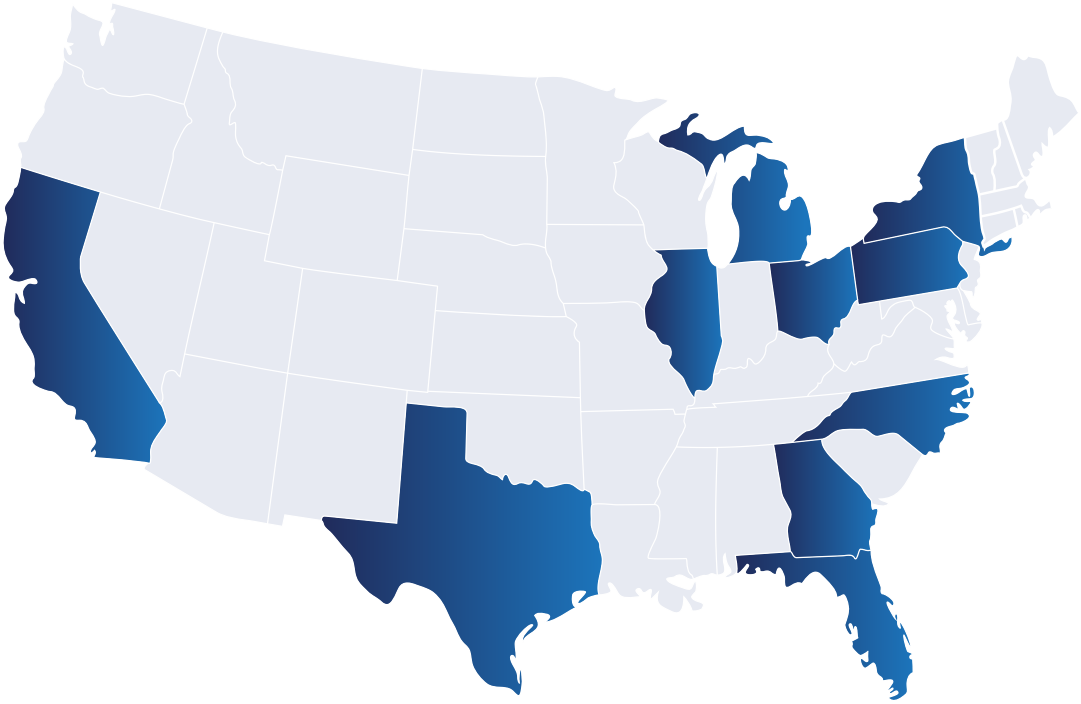
Victims Reporting Identity Misuse by Type by State

	Crime Committed Using Pii	*Existing Account Takeover*	*False Employment*	*New Account Created*	*State Totals*
Alabama	1	26	2	20	***50***
Alaska	1	5	0	5	***11***
Arkansas	3	23	0	9	***35***
Arizona	5	48	8	27	***88***
California	30	473	34	271	***825***
Colorado	2	48	4	30	***86***
Connecticut	2	38	1	25	***68***
District of Columbia	0	4	1	10	***15***
Delaware	1	9	0	15	***26***
Florida	6	217	4	109	***343***
Georgia	8	93	0	55	***159***
Hawaii	0	15	0	3	***18***
Iowa	2	24	1	8	***35***
Idaho	0	10	0	7	***17***
Illinois	8	102	7	78	***198***
Indiana	2	58	0	24	***84***

	Crime Committed Using Pii	Existing Account Takeover	False Employment	New Account Created	State Totals
Kansas	1	9	0	14	***24***
Kentucky	4	32	1	17	***54***
Louisiana	2	34	0	23	***59***
Massachusetts	3	63	2	17	***85***
Maryland	4	67	1	27	***99***
Maine	2	13	0	7	***23***
Michigan	3	64	3	52	***123***
Minnesota	4	35	0	13	***53***
Missouri	3	34	3	14	***60***
Mississippi	0	17	1	16	***36***
Montana	1	8	0	1	***10***
North Carolina	4	91	4	43	***143***
North Dakota	0	1	0	1	***2***
Nebraska	0	7	0	1	***9***
New Hampshire	0	13	0	2	***15***
New Jersey	6	91	1	32	***130***
New Mexico	3	36	2	50	***91***
Nevada	2	34	1	23	***62***
New York	10	225	6	120	***368***
Ohio	11	77	0	45	***136***
Oklahoma	4	26	0	16	***46***
Oregon	2	39	0	20	***63***
Pennsylvania	4	122	3	85	***215***
Rhode Island	1	7	1	3	***12***
South Carolina	8	27	2	24	***62***
South Dakota	0	0	0	3	***3***
Tennessee	5	54	0	58	***118***
Texas	28	235	12	132	***414***
Utah	0	27	2	10	***40***
Virginia	3	67	2	34	***108***
Vermont	0	6	0	4	***10***
Washington	7	48	1	42	***98***
Wisconsin	0	23	2	17	***44***
West Virginia	2	7	0	4	***13***
Wyoming	0	13	0	2	***15***
Totals	***198***	***2,845***	***112***	***1,668***	***4.901***

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* ***893***
2. *Texas* ***535***
3. *Florida* ***475***
4. *New York* ***434***
5. *Pennsylvania* ***262***
6. *Illinois* ***246***
7. *Michigan* ***231***
8. *North Carolina* ***224***
9. *Ohio* ***223***
10. *Georgia* ***212***

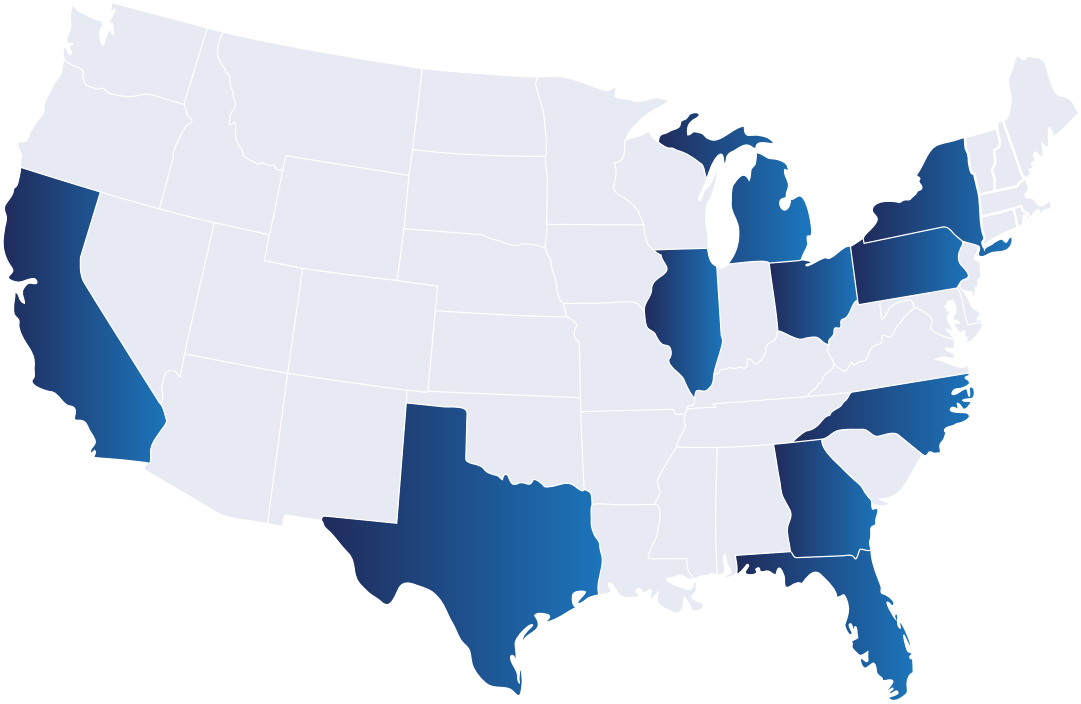
Victims Reporting Identity Compromises by Type by State

	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*	***State Totals***
Alabama	0	3	1	9	2	0	59	7	***81***
Alaska	0	0	0	0	0	0	13	1	***14***
Arkansas	2	1	0	2	2	1	51	2	***61***
Arizona	7	0	0	12	5	1	108	9	***143***
California	26	1	5	158	14	10	607	65	***893***
Colorado	3	2	0	15	1	1	110	5	***138***
Connecticut	1	0	0	4	1	0	74	3	***83***
District of Columbia	0	0	0	0	3	0	13	1	***18***
Delaware	0	0	0	4	0	0	30	0	***34***
Florida	8	1	0	39	3	1	400	20	***475***
Georgia	8	1	0	16	5	2	167	12	***212***
Hawaii	0	0	0	1	0	0	30	0	***31***
Iowa	2	0	0	8	1	0	63	7	***82***
Idaho	0	0	0	3	0	0	28	1	***32***
Illinois	5	2	1	19	5	0	200	12	***246***
Indiana	1	0	0	8	3	0	109	6	***127***

	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	State Totals
Kansas	2	1	0	3	1	0	40	0	***47***
Kentucky	6	0	0	10	0	1	57	4	***78***
Louisiana	1	2	0	14	0	0	52	8	***77***
Massachusetts	3	1	0	8	3	1	123	5	***144***
Maryland	0	0	0	6	1	1	107	5	***121***
Maine	0	0	0	2	0	0	25	1	***28***
Michigan	5	0	0	13	1	1	203	6	***231***
Minnesota	6	0	0	10	5	1	116	11	***150***
Missouri	3	0	1	12	1	0	115	2	***135***
Mississippi	4	0	0	2	1	0	45	0	***53***
Montana	0	0	0	1	2	0	19	0	***23***
North Carolina	4	0	0	20	2	1	185	10	***224***
North Dakota	0	0	0	0	1	0	9	0	***10***
Nebraska	0	0	0	1	0	0	32	0	***33***
New Hampshire	1	0	0	1	0	0	23	2	***27***
New Jersey	2	0	0	12	3	2	159	8	***186***
New Mexico	4	2	0	15	1	1	43	3	***69***
Nevada	1	0	0	8	2	1	59	6	***77***
New York	12	3	1	46	8	2	341	18	***434***
Ohio	6	0	1	16	2	4	185	8	***223***
Oklahoma	1	0	0	9	0	2	65	1	***78***
Oregon	10	0	1	11	3	0	80	7	***112***
Pennsylvania	9	0	0	17	3	0	222	10	***262***
Rhode Island	0	0	0	2	0	0	19	0	***21***
South Carolina	3	1	0	11	0	0	90	7	***112***
South Dakota	1	0	0	2	0	0	11	1	***15***
Tennessee	6	0	1	9	1	1	119	10	***149***
Texas	13	5	0	80	11	5	397	22	***535***
Utah	1	0	0	1	1	0	41	4	***48***
Virginia	6	1	0	9	0	1	132	6	***157***
Vermont	0	0	0	1	0	0	12	1	***14***
Washington	5	2	0	11	2	1	130	10	***163***
Wisconsin	3	2	0	3	1	0	101	3	***114***
West Virginia	0	1	0	5	0	0	26	3	***35***
Wyoming	0	0	0	1	0	0	9	0	***10***
Totals	***181***	***32***	***12***	***670***	***101***	***42***	***5,454***	***333***	***6,868***

Scam by State

Top 10 States by Total Victims Reporting Identity Scam



Top 10 States by Total Victims Reporting Identity Scam

1.	*California*	***614***
2.	*Texas*	***402***
3.	*Florida*	***394***
4.	*New York*	***345***
5.	*Pennsylvania*	***215***
6.	*Illinois*	***205***
7.	*Michigan*	***201***
8.	*Ohio*	***188***
9.	*North Carolina*	***183***
10.	*Georgia*	***166***

Victims Reporting Identity Scam by State, Part 1

	Amazon	Bitcoin	Google Voice	Government Grant	Job/Employment	Lottery/Prize	Phony Business or Organization	Phony Financial Account	Phony Government Agency
Alabama	2	1	33	1	4	7	1	1	3
Alaska	0	0	9	0	0	0	1	1	1
Arkansas	1	0	32	2	1	6	3	1	0
Arizona	4	3	64	3	3	6	11	4	3
California	17	26	292	16	38	23	62	10	51
Colorado	2	2	80	1	2	5	2	0	5
Connecticut	0	1	47	3	3	2	6	0	5
District of Columbia	0	0	9	0	0	0	0	1	0
Delaware	2	0	20	0	1	0	1	1	2
Florida	11	3	253	13	11	21	28	3	19
Georgia	2	2	95	6	10	8	14	1	10
Hawaii	3	1	16	0	0	1	4	2	2
Iowa	0	0	43	2	2	2	3	0	2
Idaho	0	1	18	0	1	1	1	0	1
Illinois	4	4	135	4	2	10	16	1	12
Indiana	1	2	77	0	1	6	0	0	3

	Amazon	Bitcoin	Google Voice	Government Grant	Job/Employment	Lottery/Prize	Phony Business or Organization	Phony Financial Account	Phony Government Agency
Kansas	1	1	25	0	0	3	1	1	3
Kentucky	1	2	36	1	3	3	1	3	4
Louisiana	1	0	30	0	1	3	6	1	6
Massachusetts	5	1	78	2	3	0	10	0	10
Maryland	1	4	64	1	5	3	9	3	11
Maine	0	1	21	1	0	0	1	0	0
Michigan	3	3	144	8	4	7	12	1	5
Minnesota	1	1	82	2	1	6	5	1	4
Missouri	1	1	77	4	2	10	5	3	3
Mississippi	0	2	25	4	1	2	1	0	1
Montana	0	0	15	0	0	1	1	0	2
North Carolina	6	2	116	4	8	12	12	1	3
North Dakota	0	0	8	0	0	1	0	0	0
Nebraska	1	0	21	0	1	2	3	0	4
New Hampshire	0	0	18	0	0	0	1	0	0
New Jersey	1	3	98	2	8	4	13	5	6
New Mexico	5	0	15	2	3	5	3	2	4
Nevada	1	3	30	2	1	7	6	0	6
New York	9	8	189	10	15	12	30	7	31
Ohio	7	4	111	6	1	10	12	4	5
Oklahoma	2	3	37	2	2	7	3	0	4
Oregon	1	0	48	1	4	2	6	2	4
Pennsylvania	1	5	146	7	8	6	12	4	7
Rhode Island	0	1	13	0	0	2	2	0	1
South Carolina	1	2	60	2	2	6	3	2	4
South Dakota	0	0	9	1	0	0	0	0	1
Tennessee	0	3	85	1	3	4	6	1	7
Texas	4	9	260	12	14	17	17	9	25
Utah	0	0	26	0	1	3	4	1	1
Virginia	1	1	93	2	5	7	9	0	7
Vermont	0	0	7	0	0	1	3	0	1
Washington	3	4	75	2	1	3	12	3	11
Wisconsin	1	0	75	3	2	4	7	0	6
West Virginia	0	0	17	1	1	2	0	1	1
Wyoming	1	1	3	0	1	0	0	1	0
Totals	***108***	***108***	***3,380***	***134***	***190***	***253***	***374***	***82***	***307***

Victims Reporting Identity Scam by State, Part 2

	Phony Law Enforcement	Rental or Purchase	Romance/Sweetheart	Tech Support	Unknown	State Totals
Alabama	0	0	2	1	2	***58***
Alaska	0	0	0	0	1	***13***
Arkansas	0	0	0	1	2	***49***
Arizona	3	0	2	1	2	***109***
California	6	16	21	8	28	***614***
Colorado	2	1	1	1	7	***111***
Connecticut	1	0	2	0	5	***75***
District of Columbia	0	0	0	0	2	***12***
Delaware	0	0	0	0	2	***29***
Florida	3	6	7	4	12	***394***

	Phony Law Enforcement	Rental or Purchase	Romance/Sweetheart	Tech Support	Unknown	State Totals
Georgia	1	4	4	2	7	***166***
Hawaii	0	0	0	1	1	***31***
Iowa	1	1	0	0	4	***60***
Idaho	1	2	1	0	1	***28***
Illinois	2	4	5	0	6	***205***
Indiana	1	3	1	0	9	***109***
Kansas	1	1	2	0	2	***41***
Kentucky	0	1	2	0	3	***60***
Louisiana	0	0	1	0	3	***52***
Massachusetts	4	2	2	2	2	***121***
Maryland	1	0	2	0	6	***110***
Maine	0	0	1	0	2	***27***
Michigan	2	3	1	1	7	***201***
Minnesota	0	2	5	1	5	***116***
Missouri	0	1	2	1	5	***115***
Mississippi	0	3	1	1	2	***43***
Montana	0	0	0	0	1	***20***
North Carolina	1	0	5	1	12	***183***
North Dakota	0	0	0	0	0	***9***
Nebraska	0	0	0	1	0	***33***
New Hampshire	0	1	1	1	1	***23***
New Jersey	2	3	4	0	9	***158***
New Mexico	0	1	1	1	1	***43***
Nevada	0	0	2	1	1	***60***
New York	2	7	8	3	14	***345***
Ohio	2	2	2	1	11	***188***
Oklahoma	0	2	1	1	1	***65***
Oregon	2	1	3	2	3	***79***
Pennsylvania	2	6	3	1	7	***215***
Rhode Island	0	0	0	0	0	***19***
South Carolina	1	0	0	1	5	***89***
South Dakota	0	0	0	0	0	***11***
Tennessee	0	3	2	1	4	***120***
Texas	3	5	6	1	20	***402***
Utah	0	0	1	1	1	***39***
Virginia	0	0	0	1	5	***131***
Vermont	0	0	0	0	0	***12***
Washington	2	3	2	1	9	***131***
Wisconsin	1	1	1	0	0	***101***
West Virginia	0	1	1	0	2	***27***
Wyoming	0	1	0	0	0	***8***
Totals	***47***	***87***	***97***	***44***	***235***	***5,460***