

2021

TRENDS

IN IDENTITY

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT
RESOURCE CENTER





Table of Contents

i. Letter from the CEO	4
ii. 2021 Summary	9
iii. 2021 Trends & Identity Statistics	12
iv. 2021 Notable Trends	21
v. Glossary of Terms	29
vi. Appendix	31

Looking back on the past year, 2021 was a record-breaking year in so many respects. For victims of identity crimes and compromises, fraud and scams reached levels never seen in any previous year since the Identity Theft Resource Center (ITRC) was founded in 1999.

In the 12 months ending on December 31st 2021, there were more data breaches reported in a single year since all 50 states and U.S. territories adopted data breach notice laws, the last two states in 2018. Identity-related unemployment benefits fraud, never much of a problem prior to the pandemic, shot to the top of the list for most reported – and most costly – government benefits fraud. Rather than take control of existing financial accounts as in years past, identity criminals preferred to open new accounts using personal information stolen in data breaches or collected from individuals tricked into sharing information with criminals.

We know all of this information because each day dozens of identity crime victims, or people seeking to avoid becoming a victim, contact the ITRC.

A record number in 2021 – just short of 15,000 people.

That doesn't count the thousands of repeat victims or victimizations carrying over from previous years.

Historically, the ITRC has never shared the information you are about to read in the pages that follow. For much of the life of the Center, we focused exclusively on providing free, direct victim assistance to identity crime victims. That is still the rock-hard foundation of what we do.

But over time, we have learned that a key to helping individuals as well as business, government, and institution leaders requires sharing knowledge. We started by sharing information about the full range of impacts of identity crimes – financial and non-financial - on victims who contacted the ITRC. That formed the basis of our [Consumer Aftermath Report](#) that continues to this day.

Next, we strongly believed there was a connection between data breaches and identity crimes. Starting in 2005, our annual **Data Breach Report** documented that link even as the nature of data breaches and the people who commit them changed. In 2021 we added the **Small Business Aftermath Report**, a first-of-its-kind analysis of the impacts identity crimes and cyberattacks have on small businesses, the life-blood of the U.S. economy.

And now we add this report – the **Trends in Identity Report** that looks at the wide range of identity crimes committed against individuals as reported by the victims of those crimes.

You'll learn first-hand of the identity scams we see and how criminals convince people to willingly share information they know should be protected. You'll read about how stolen information is being used to open new bank and other accounts in the name of individuals who have no idea their good name is being used as part of a fraudulent scheme. And, you'll see the words of victims and the advice the ITRC shares on how to protect yourself and your information to reduce the impact of identity crimes.

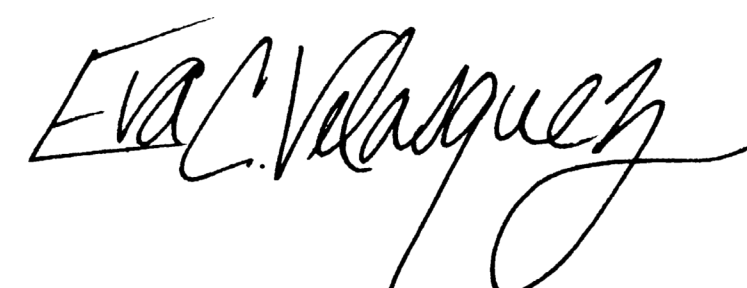
If this is your first time learning of the ITRC and our work, I encourage you to learn more about how we are the only national organization that provides direct assistance, free

of charge, to individual identity crime victims. Visit our website, where you will also learn how to create a [data breach alert](#) for yourself in the event an organization where you have a relationship issues a breach notice that may or may not be delivered to you directly.

[Our website](#) is filled with other valuable information for individuals and organizations about identity crimes, privacy and data protections, and identity-related issues. I hope you will find the information 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 C. Velasquez



(President & CEO, ITRC)

August 2022



For victims of identity crimes and compromises, **fraud and scams** reached levels never seen in any previous year since the Identity Theft Resource Center (ITRC) was founded in 1999.

The *Trends in Identity Report* looks at the wide range of identity crimes committed against individuals as reported by the victims of those crimes. Get it at www.idtheftcenter.org/publications/



14,947 contacts

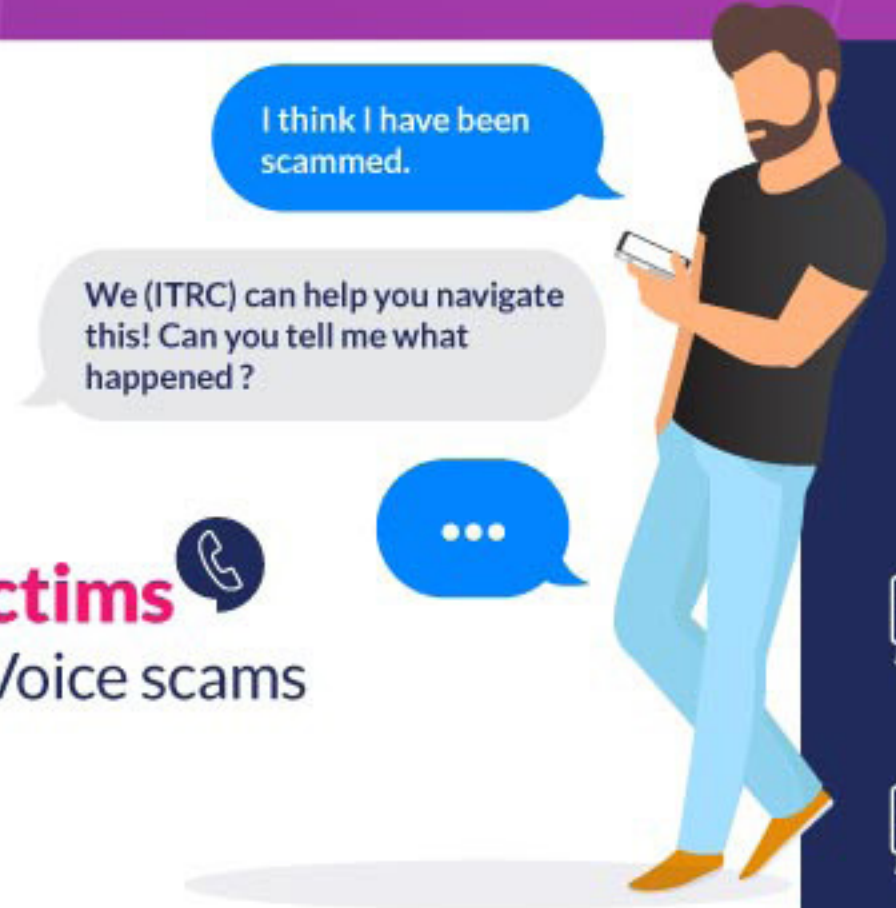
ITRC reported a record number contacts in 2021
(A 36% increase from 2020)



7,412 scam victims
Victims reported sharing Personally Identifiable Information (PII) with criminals



3,925 victims
of Google Voice scams



Identity criminals don't target any one demographic - age, wealth, location, and living status don't matter.



4,168 identity misuses

ITRC reported a steady increase in new account fraud in 2021
(An 8% increase from 2020)



1,681 victims
of financial account misuse



2,270 cases
of PII used to open, access, takeover or apply for government benefits



One victim received a notice that someone tried applying for a credit card with his **child's information**.



"I provided a **picture of my passport** to a company offering free grants."



A victim received a letter from an unemployment office under her **deceased husband's name** who had passed nine years prior.



A representative from a homeless shelter contacted the ITRC with a victim on the line who was applying for food stamps and was denied because the benefits office said the victim had received **\$10,000 in unemployment funds**.

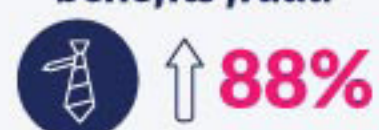


"The SBA has been sending me **monthly notices** since October 2020 that I owe them \$9,900 for a disaster loan. I have made many reports to numerous agencies to no avail."

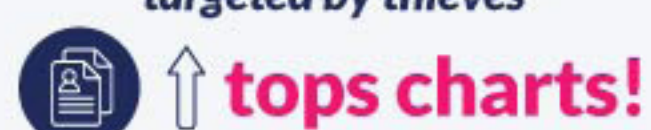
Social media account hijacking



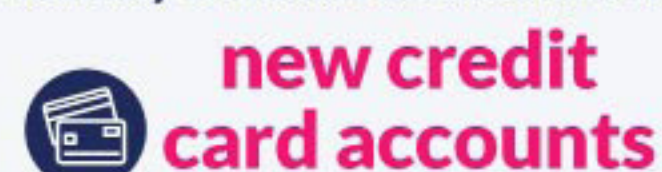
Unemployment benefits fraud



Pandemic-related fraud targeted by thieves



Identity criminals used stolen PII to open



2021 Summary



14,947 contacts

In 2021, the ITRC received the highest number of contacts in its history about identity crimes and requests for assistance to prevent identity misuse.

ITRC | IDENTITY THEFT
RESOURCE CENTER

2021
TRENDS
IN IDENTITY

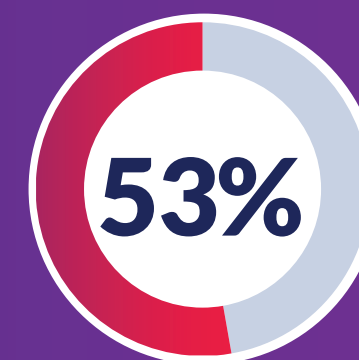


7,412 victims

Identity scams were the primary cause of individual victims sharing Personally Identifiable Information (PII) with criminals.

ITRC | IDENTITY THEFT
RESOURCE CENTER

2021
TRENDS
IN IDENTITY



3,925 victims

Google Voice scams were the most reported identity-related scams.

ITRC | IDENTITY THEFT
RESOURCE CENTER

2021
TRENDS
IN IDENTITY

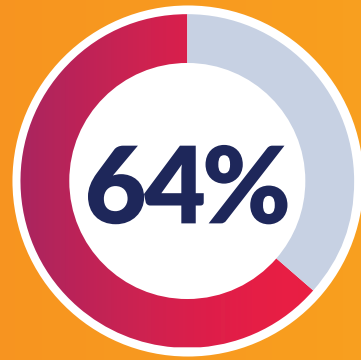




1,127 victims of financial account misuse was due to new account fraud

ITRC | IDENTITY THEFT RESOURCE CENTER

2021 TRENDS
IN IDENTITY

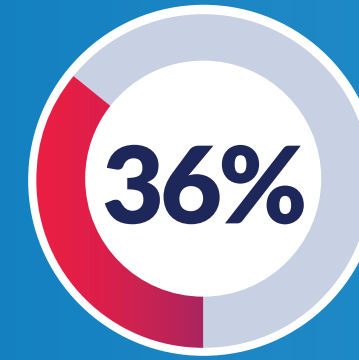


New account fraud



ITRC | IDENTITY THEFT RESOURCE CENTER

2021 TRENDS
IN IDENTITY



Existing account takeover (ATO)



ITRC | IDENTITY THEFT RESOURCE CENTER

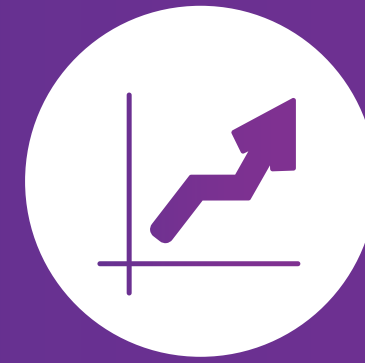
2021 TRENDS
IN IDENTITY





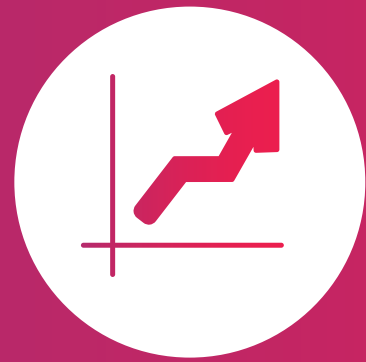
235% increase

Reports from victims of non-financial account takeover increased 235% over 2020.



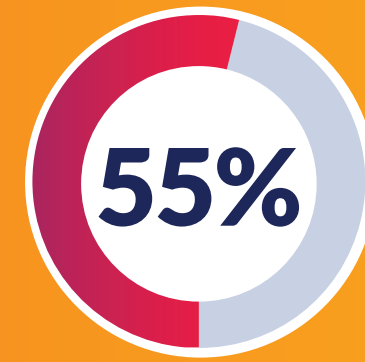
1,044% increase

Social media account takeover grew 1,044% from 2020 to 2021.



154% increase (2019 - 2020)
7% increase (2020 - 2021)

Overall identity misuse involving government credentials or accounts.



2,270 cases of identity misuse reported

Involved the use of PII or government credentials to open, access, take over government accounts, or apply for benefits.

6,085% increase | Unemployment accounts 2019 - 2020

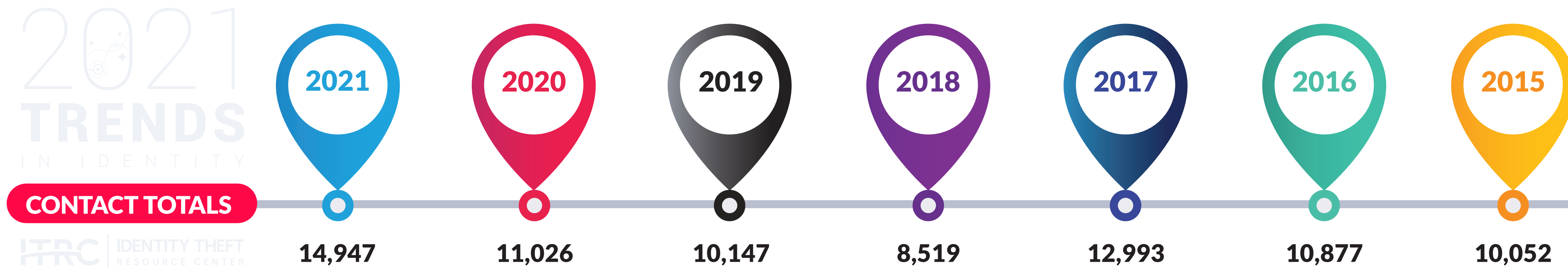
88% increase | Unemployment accounts 2020 - 2021

32% increase | Fraudulently filed taxes with the IRS 2020 - 2021

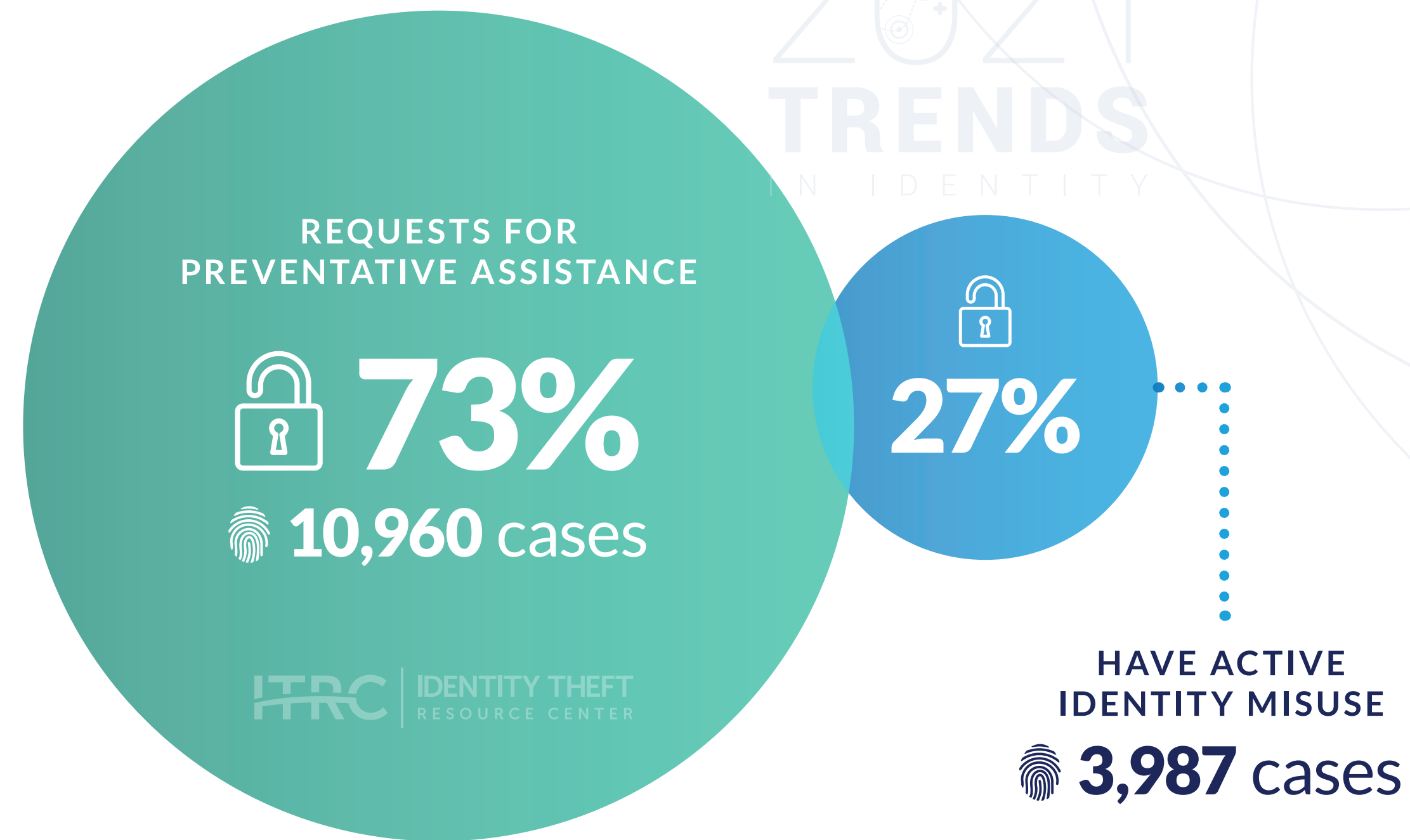


2021 Trends & Identity Statistics

In 2021, the ITRC had the highest number of reported identity crimes (compromises, theft, and misuse) in the ITRC's history:



Victims most frequently requested assistance with preventative steps and/or compromised PII.



Root of Compromise

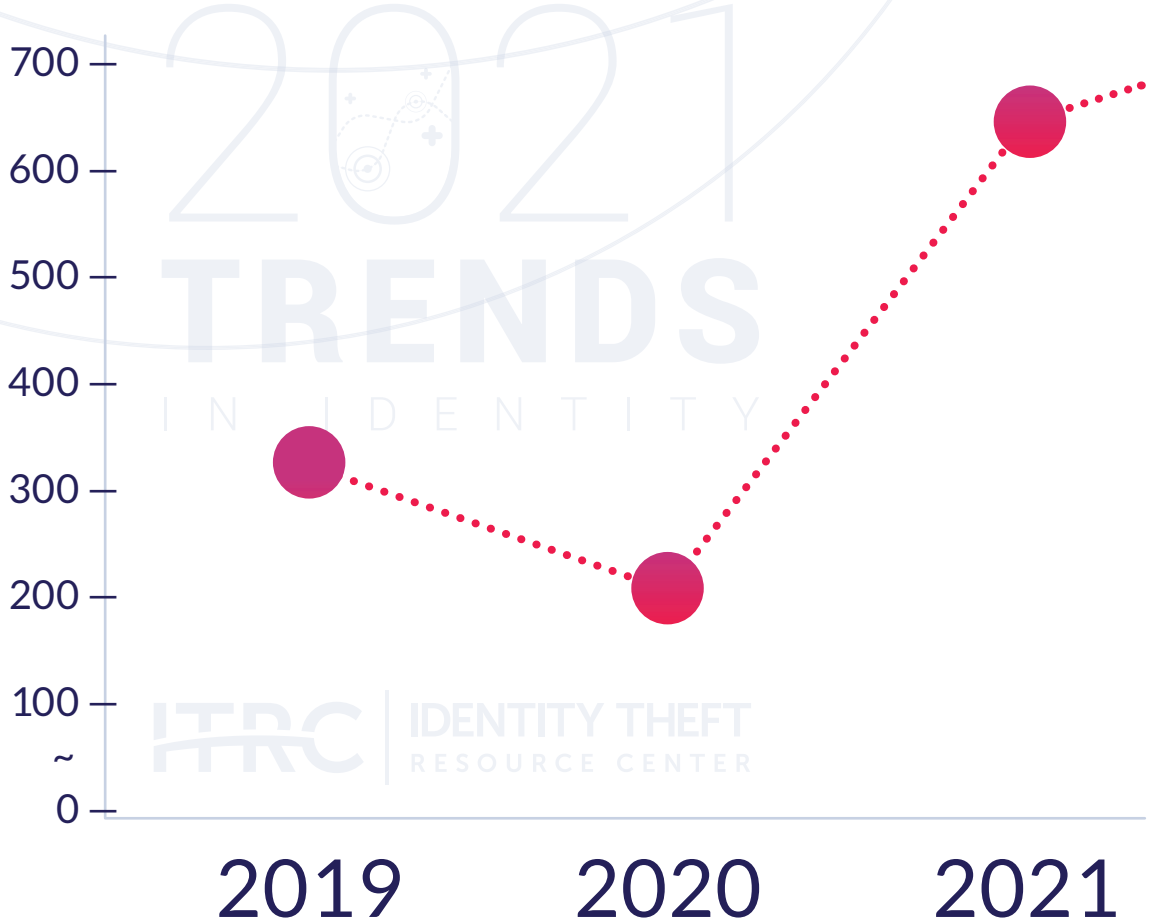
Non-financial account takeover trends:

-  **331** cases in 2019
-  **202** cases in 2020
-  **677** cases in 2021

 **1,044% increase**
Hijacked social media accounts

 **34% increase**
Mobile device compromises

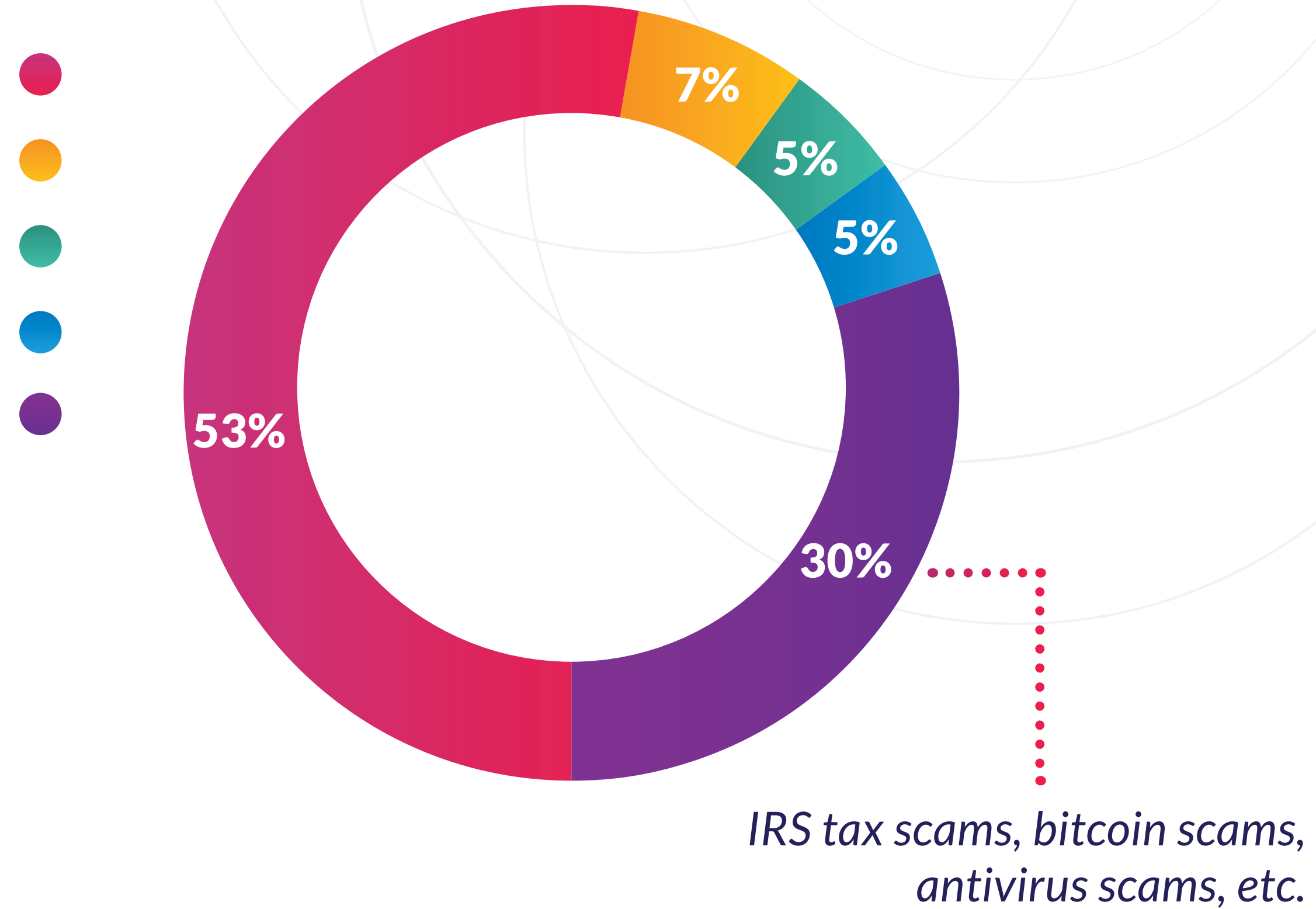
 **76% increase**
Compromised email accounts



Root of Compromise

Scams

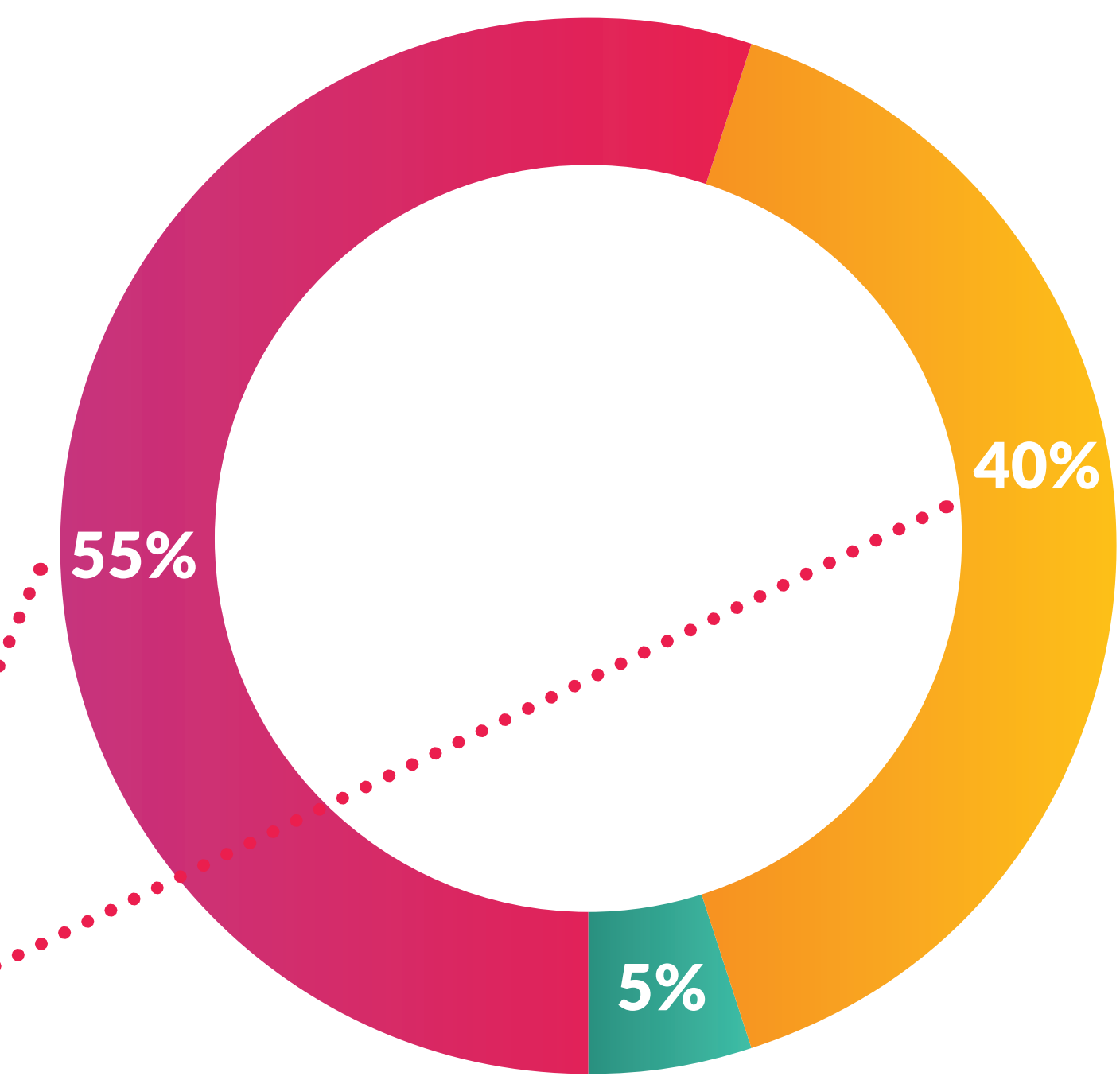
	/ Qty	/ %
Google Voice	3,925	53%
Government Grants	531	7%
Phony Government Agencies	376	5%
Job/Employment Scams	366	5%
Other	2,214	30%






Root of Compromise

Top accounts compromised by identity misuse:

	Qty	%
Open/access/takeover Government accounts/benefits	2,270	55%
Misuse of credentials to access/ create financial accounts	1,681	40%
Non-financial	217	5%






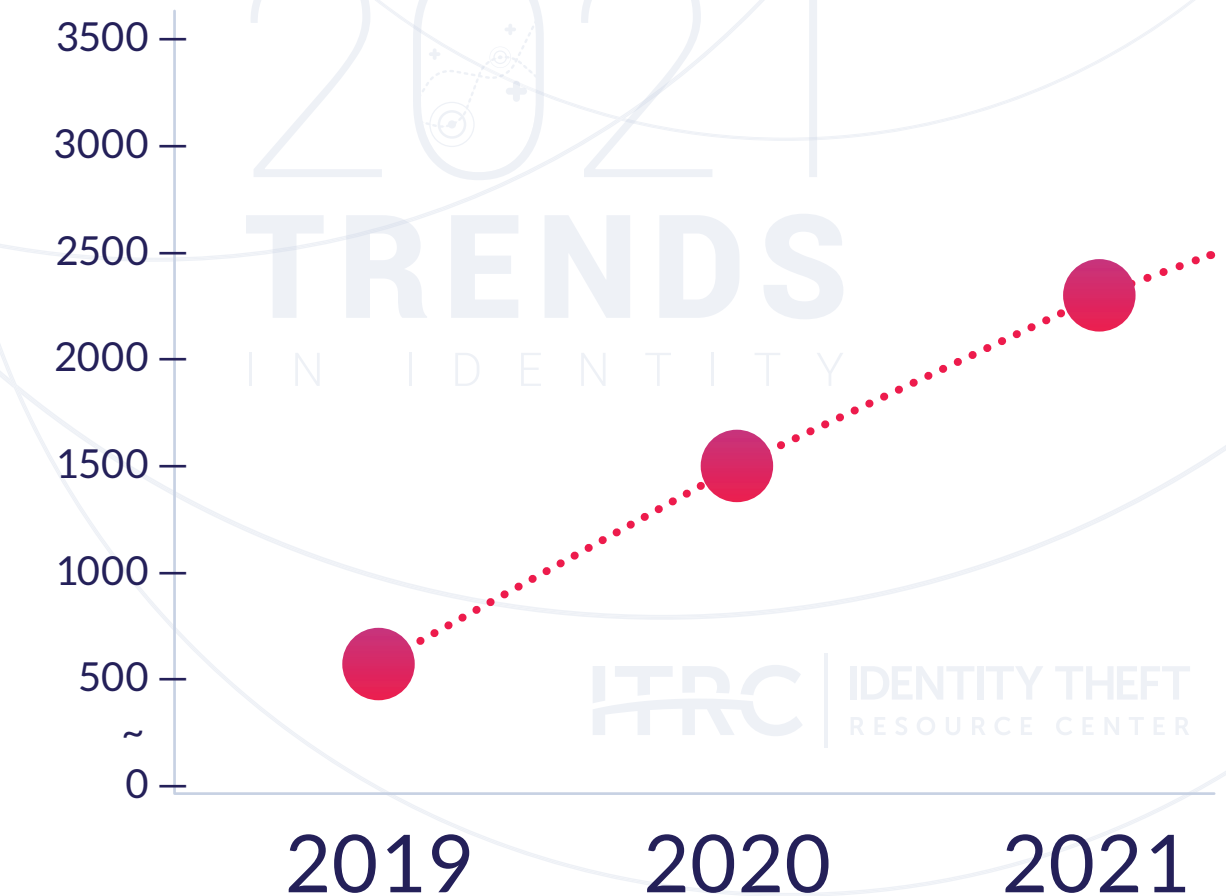
-  Unemployment, SBA/PPP Loan, IRS, etc.
-  Checking/savings accounts, credit cards
-  Medical accounts, etc.

Root of Compromise

Government Scams

Identity misuse involving government credentials/accounts 3 year review:

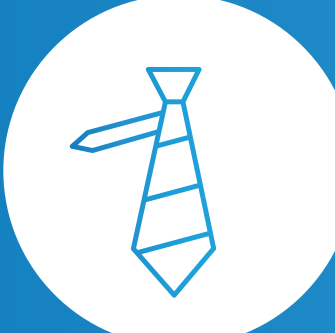
-  **5.6%** total cases (2019)
-  **14.2%** total cases (2020)
-  **15.2%** total cases (2021)




Root of Compromise

Government Scams

2021 government identity misuse trends:



86% of government benefit fraud is related to unemployment.



ITRC | IDENTITY THEFT RESOURCE CENTER



288% increase in SBA loan misuse. This grew 4,000% from 2018 to 2020.



ITRC | IDENTITY THEFT RESOURCE CENTER



32% increase in fraudulently filed taxes.

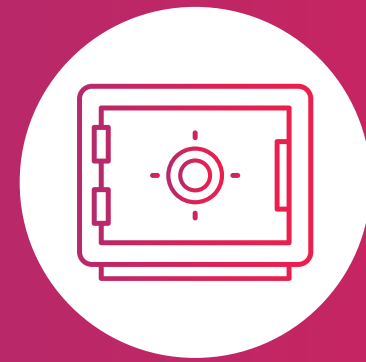


ITRC | IDENTITY THEFT RESOURCE CENTER

Root of Compromise

Financial Account Scams

Financial account identity misuse trends:



37% of all account takeovers were bank accounts/financial accounts.

ITRC | IDENTITY THEFT
RESOURCE CENTER

2021
TRENDS
IN IDENTITY



36% of new account fraud was credit card accounts.

ITRC | IDENTITY THEFT
RESOURCE CENTER

2021
TRENDS
IN IDENTITY



8% increase in new account fraud due to new accounts being opened.

ITRC | IDENTITY THEFT
RESOURCE CENTER

2021
TRENDS
IN IDENTITY

Notable Trends

- 1 The Emerging Scamdemic** | How identity thieves flocked to social media in a scamdemic of account takeover. How to stay vigilant.
- 2 The Opportunistic Thief** | Learn how pandemic-related assistance was targeted heavily by thieves. Get the scoop!
- 3 New Accounts on the Rise** | Trending data shows the number of new financial accounts being opened in a victim's name increased in 2021. What can be done?

1 The Emerging Scamdemic

How identity thieves flocked to social media in a scamdemic of account takeover.

In 2021, the highest number of PII exposures/compromises or attempted compromises was due to scams on social media platforms based on social engineering techniques. Social media accounts were the most reported account affected by non-financial account takeover as a result of three primary scams.

What happened:

Beginning in the last quarter of 2021, the ITRC received a large influx of contacts selling items on online marketplaces using Google Voice numbers as part of their business. Scammers leveraged the desire of victims to prove they were legitimate sellers by asking the victim to share a verification code for Google Voice. Criminals obtain Google Voice phone numbers with a U.S. area code to sell the number outside the country or to perpetrate other scams linked to the victim's legitimate Google Voice number.

Other contacts reported receiving a direct message from a "friend," letting them know that the "friend" was a recipient of a grant from the government and they should also apply by sharing their address, date of birth, driver's license information, and/or paying a fee to obtain the money.

Hacked/taken-over social media accounts, specifically Instagram accounts, were reported to the ITRC by many social media influencers who were lured into phishing scams with claims they could increase the likelihood of their account being verified on Instagram’s platform. Others were told they could make money on a bitcoin investment and were told to record a video and post it, stating they made money even though they hadn’t. Victims of both scams were asked to provide account details that allowed a scammer to take control of an account. In all instances, the recovery number/email for the social media account was changed, and the victims were locked out of their accounts.

Victims reported:



– ITRC Victims –

“I’m selling a listing on Facebook Marketplace for the first time and got a message asking to give my phone number so they can verify I was real. I fell for it and sent them back the Google Voice code they sent. What do I do?”

“I provided a picture of my passport to a company offering free grants. It is a scam.”

“My account was hacked after I chatted with someone who told me to change my email address in my account so I can be verified.” Upon reaching out to the victim, our advisor was informed that the person who hacked the account was chatting with the victim about Bitcoin sales. The victim sent no money but was told to create a video stating he received 500.00 from the bitcoin sale. He never made a video.

How to stay vigilant:



Watch out for direct/private messages from “friends” and followers stating you can win or earn money easily.

The adage “if it is too good to be true, then it probably is” is usually accurate. Hackers/scammers have gotten good at taking over accounts or spoofing legitimate accounts, so you can’t rely on the person “talking” to you by chat actually being your friend.



Don’t click on links.

If you want to investigate something sent to you, look it up separately from a trusted/reliable source.



Don’t share personally information until you verify the person/company making the offer/request is who they claim to be.

Driver’s license information, passport numbers, logins and passwords, one time passwords and MFA codes, account numbers, etc., should remain private. Ask why your information is needed before you share it and be prepared to say no!

2 The Opportunistic Thief

Pandemic-related assistance was targeted heavily by thieves.

Pandemic-related payments were the most reported stolen item. Government benefits/accounts related to the pandemic (unemployment insurance benefits, SBA loans, PPP loans, cash benefits) made up the highest number of accounts reported as misused.

What happened:

Stimulus payments and Child Tax Credit payments were reported as stolen either through the mail or through an unauthorized account takeover where the bank account information was changed at the IRS portal, or the money was taken from the account where the money was deposited. Unfortunately, many who reported the account takeover knew or had an idea of who the thief was, and it tended to be a spouse, ex-spouse, or family member.

The highest reported misuse of credentials was to open, access, or takeover government accounts/benefits (unemployment insurance, SBA loans, PPP loans, cash benefits) that were enhanced due to the pandemic. Victims found out that unemployment accounts had been opened in their name primarily through four methods:

- + **Denied unemployment benefits** due to previous claims by someone using a stolen identity.
- + **Receipt of an unemployment award letter** or debit card in the mail.

- + **Receipt of a Form 1099-G** listing the unemployment funds that were distributed for use claiming benefits as income.
- + **Their respective employers were asked to verify their employment had been terminated.** Thieves used personal information stolen in data breaches deceased as well as compromised identities from children and the deceased to claim these benefits. Victims faced numerous hardships trying to resolve these matters.

Victims reported:



A victim's ex-wife accessed his IRS account and changed the bank account listed for direct deposit.

A representative from a homeless shelter contacted the ITRC with a victim on the line who was applying for food stamps and was denied because the benefits office said the victim had received \$10,000 in unemployment funds.

A victim received a letter from an unemployment office under her deceased husband's name who had passed nine years prior.

A victim received an unemployment letter in the name of their 9-year-old child.

"The SBA has been sending me monthly notices since October 2020 that I owe them \$9,900 for a disaster loan. I have made many reports to numerous agencies to no avail."

How to stay vigilant:



Freeze your credit report.



Guard your personally identifiable information (logins & passwords, social security number, driver's license, etc.) and do not share the information unless absolutely necessary.



Use strong, unique passcodes (one for each account), multi-factor authentication is enabled, and do not share with anyone.



Use a password manager or the password feature in mainstream browsers to create & remember passwords. Do not use the "remember my password" feature on a website.



Check your credit reports regularly for any activity that does not belong there, including hard inquiries for credit that are not from existing creditors and were not initiated by you.



Watch the mail for correspondence from government agencies and lenders and review it thoroughly so you can act if needed.

3 New Accounts on the Rise

The number of new financial accounts being opened in a victim's name increased in 2021.

Though there was an overall decrease in the number of identity misuse cases involving financial accounts from 2020 to 2021, there were more new financial accounts opened in a victim's name versus thieves accessing existing financial accounts.

What happened:

The ITRC saw a steady increase year over year in the percentage of new account fraud primarily due to new credit card accounts. This trend is disturbing because existing account takeover is more easily detected by victims and easier to dispute than new account fraud, particularly new account fraud involving bank accounts.

With financial institutions closing physical locations due to the pandemic, it was common for financial institutions to accept online applications to open new accounts in 2021. Thieves were busily using/gathering PII (Trend #1) to be able to “prove” that they were someone else. Bank accounts opened in a victim's name allowed the thieves who were obtaining funds fraudulently in that victim's name (Trend #2) to deposit the money received and then transfer it to another account. Many victims received letters of denial of credit for accounts they never attempted to open.

Victims reported:



One victim contacted the ITRC about accounts opened with four different banks.

One victim received notice that someone tried applying for a credit card with his child's information.

How to stay vigilant:



Check your credit reports regularly for any activity that does not belong there, including hard inquiries for credit that are not from existing creditors and were not initiated by you.



Freeze your credit report.



Guard your personally identifiable information (logins & passwords, social security number, driver's license, etc.) and do not share the information unless absolutely necessary.



Contact check reporting companies for any potential bank accounts opened in your name with negative activity and freeze the reports with the check reporting companies if possible.



“Each day dozens of identity crime victims, or people seeking to avoid becoming a victim, contact the ITRC.”

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 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.

+ 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).

Appendix

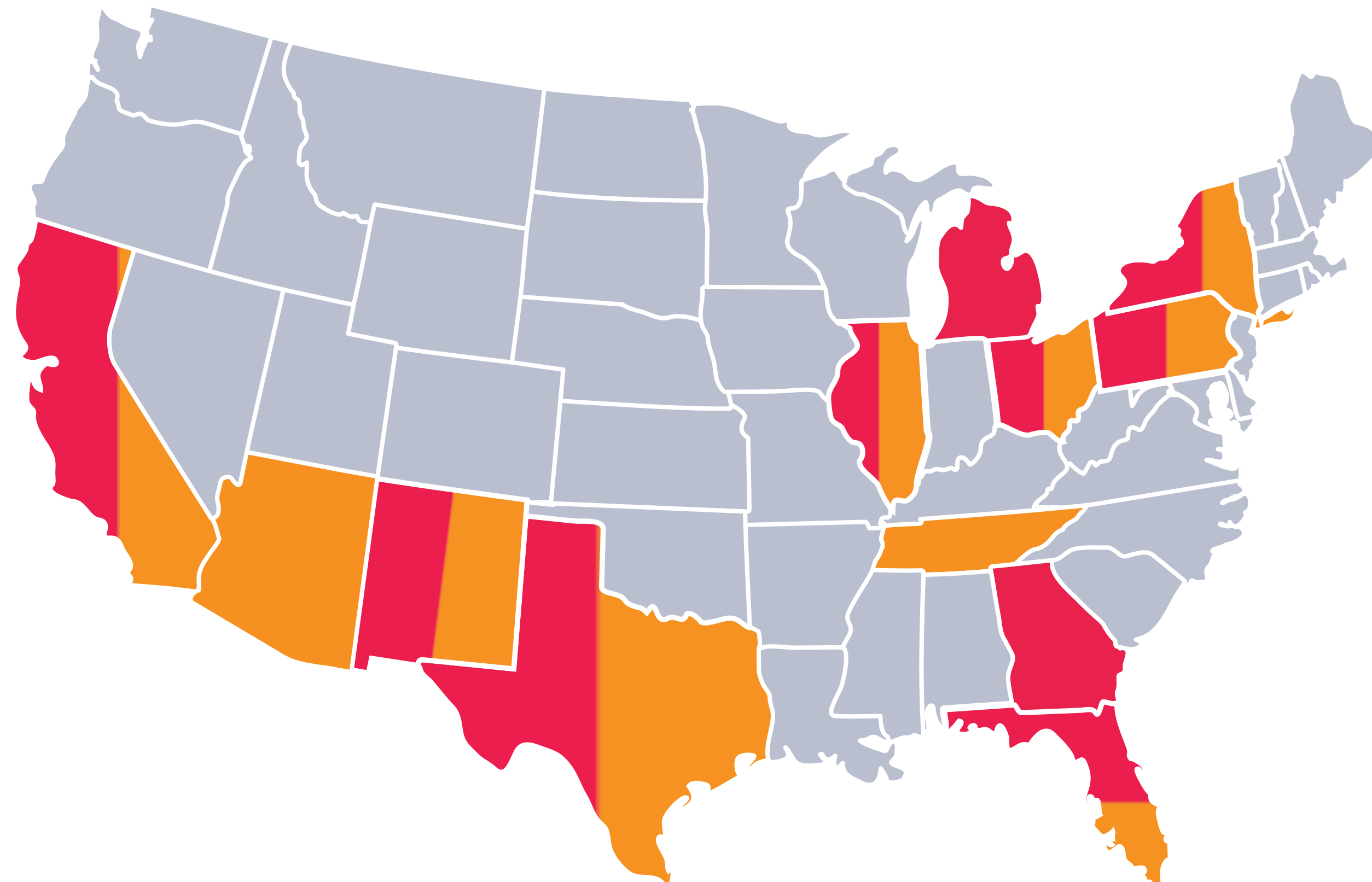
Top 10 states with:

VICTIMS WHO REQUESTED ITRC SUPPORT ●

BOTH ●

VICTIMS WHOSE PII WAS MISUSED ●

1. California	11.0%
2. Texas	7.1%
3. Florida	5.8%
4. New York	5.5%
5. Pennsylvania	4.7%
6. Illinois	3.6%
7. Ohio	3.6%
8. Michigan	3.0%
9. New Mexico	2.9%
10. Georgia	2.8%

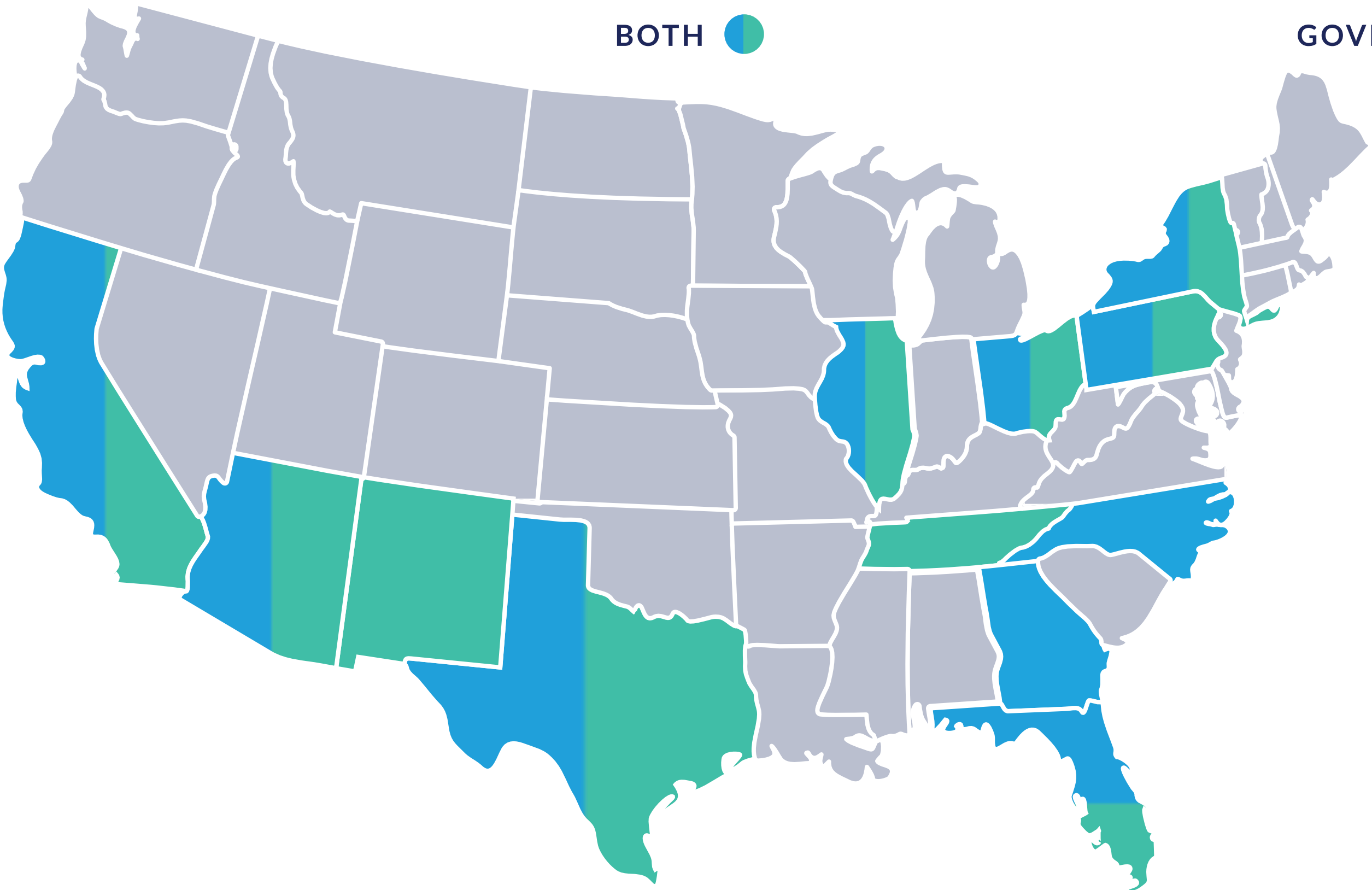


1. California	13.2%
2. New Mexico	8.9%
3. Pennsylvania	7.0%
4. New York	6.3%
5. Texas	6.3%
6. Florida	5.9%
7. Ohio	4.9%
8. Illinois	3.3%
9. Arizona	2.8%
10. Tennessee	2.8%

Top 10 states with victims reporting misuse of:

FINANCIAL ACCOUNTS ●

1. California	18.3%
2. Texas	8.1%
3. Florida	7.1%
4. New York	6.7%
5. Pennsylvania	4.0%
6. Ohio	3.6%
7. Georgia	2.9%
8. North Carolina	2.9%
9. Illinois	2.6%
10. Arizona	2.4%



GOVERNMENT CREDENTIALS/ACCOUNTS ●

1. New Mexico	15.2%
2. Pennsylvania	9.6%
3. California	9.3%
4. New York	6.0%
5. Ohio	5.9%
6. Florida	5.0%
7. Texas	4.4%
8. Illinois	4.1%
9. Tennessee	3.7%
10. Arizona	3.3%

2021

TRENDS

IN IDENTITY

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT
RESOURCE CENTER

