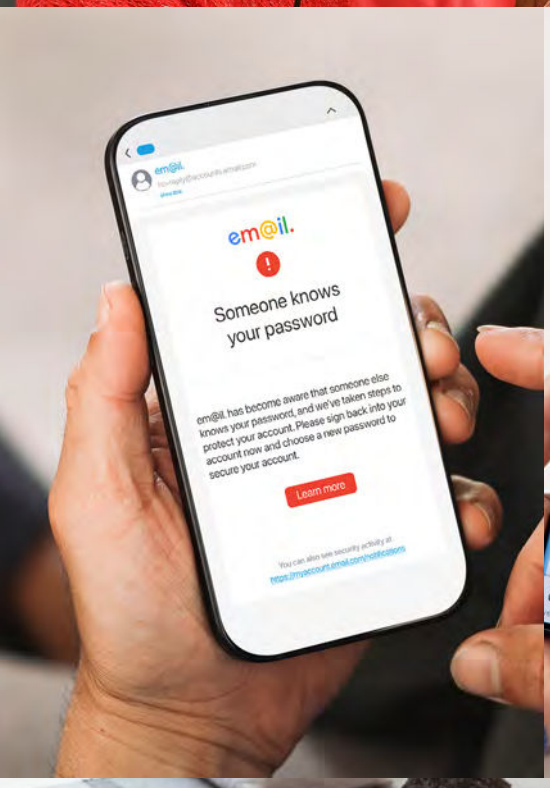
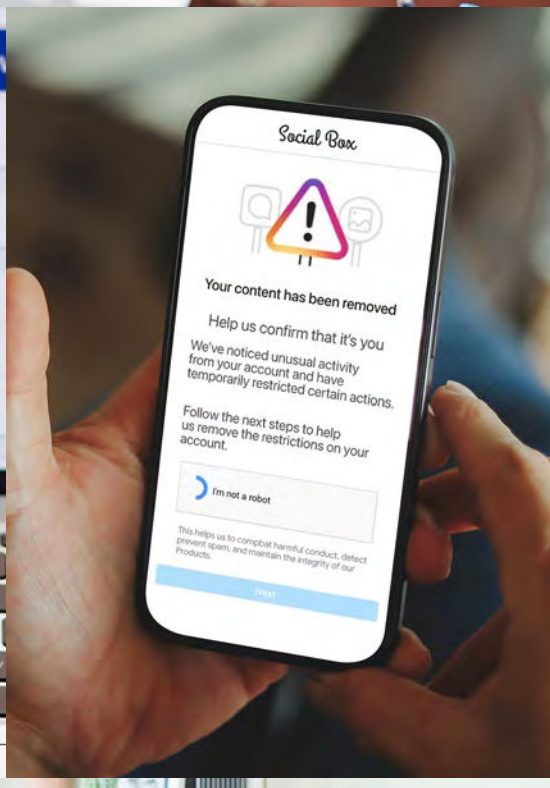
TIR

IDENTITY THEFT RESOURCE CENTER

2026 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 2026

CONTENTS

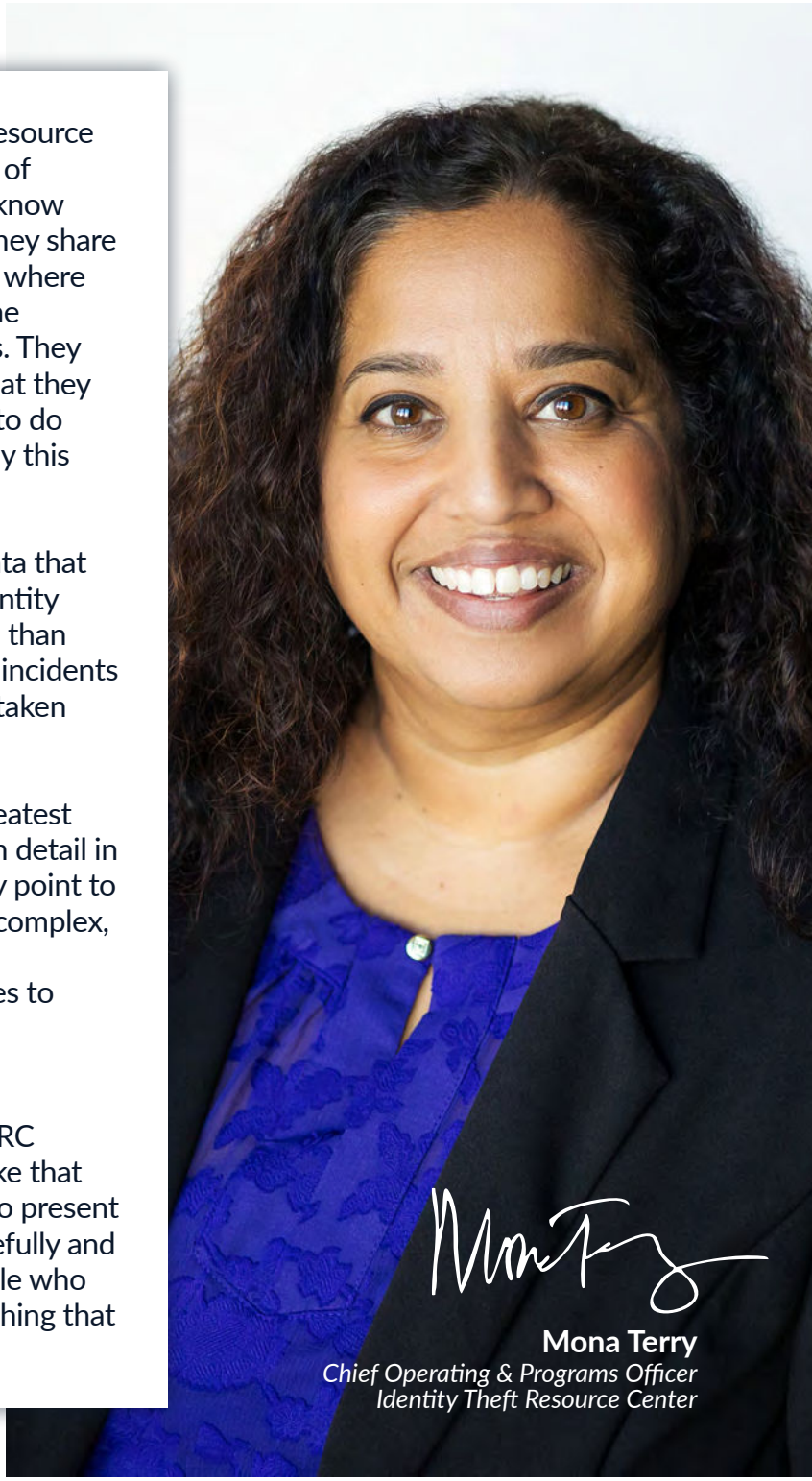
INTRODUCTION

From the Chief Operating & Programs Officer

When someone contacts the Identity Theft Resource Center (ITRC), they are often navigating a mix of confusion, frustration and uncertainty. Some know exactly what happened. Many do not. What they share with us is that they feel overwhelmed, unsure where to start and, in many cases, unsupported by the institutions they contacted before reaching us. They are looking for someone who understands what they are facing and can help them figure out what to do next. That is why we do this work, and it is why this report matters.

This year, three patterns emerged from our data that I believe will shape the identity landscape. Identity crimes are becoming multi-layered, with more than one in four individuals managing two or more incidents at once. Unauthorized device access has overtaken scams as the primary compromise method for working-age adults. And the recovery system continues to fail the people who suffer the greatest financial harm. These patterns are discussed in detail in the pages that follow, but taken together, they point to a clear shift: identity crime is becoming more complex, harder to detect and more difficult to resolve, particularly for those with the fewest resources to respond.

Every finding in this report is grounded in the experiences of real people who trusted the ITRC enough to share what happened to them. I take that trust seriously, and it carries a responsibility: to present their data accurately, to draw conclusions carefully and to use what we learn to better serve the people who come to us next. It is the foundation of everything that follows.



Mona Terry
Chief Operating & Programs Officer
Identity Theft Resource Center

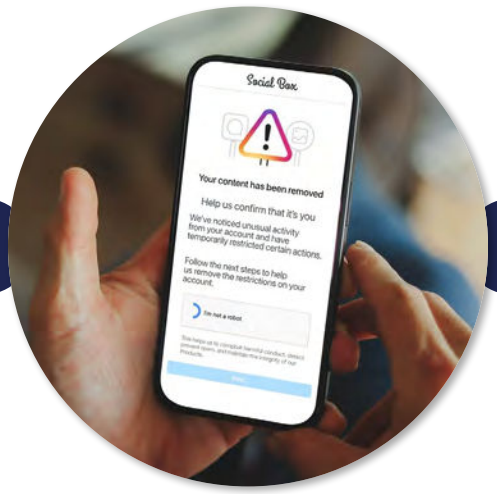
TRENDS *Defining Identity Crime*

Each year, the data reported to the ITRC reveals not just what is happening, but how identity crime is evolving. This year, three patterns emerged that we believe will shape the identity landscape. These aren't predictions – they are patterns we are seeing now, grounded in the experiences of the 6,188 individuals who contacted us during this reporting period.

TREND 1 *Identity Crimes are Becoming Multi-Layered*

Identity theft used to look like a single event: a stolen credit card number, a fraudulent charge, a compromised account. That picture is changing. More than one in four individuals (25.6%) who contacted the ITRC this year were dealing with two or more identity incidents, up from 23.5 percent (23.5%) the prior year. Nearly six percent (6%) were managing four or more.

What's significant isn't just the volume; it's the pattern. When we look at individuals based on how many incidents they faced, the nature of the crime changes at every level. Among individuals with a single incident, 18 percent (18%) experienced account takeover. Among those with two incidents, that number jumps to 51 percent (51%). At three incidents, 68 percent (68%). At four or more, 80 percent (80%). Unauthorized device access follows a similar path, rising from six percent (6%) for single-incident individuals to 40 percent (40%) for those with four or more.



This tells us that identity crime is no longer a one-and-done event for a growing number of people. A single compromise, a breached database, a stolen phone, a successful scam, can set off a chain of misuse that spreads across multiple accounts and institutions. The most common multi-incident profile in our data is account takeover combined with unauthorized device access: 178 individuals experienced this exact pairing.

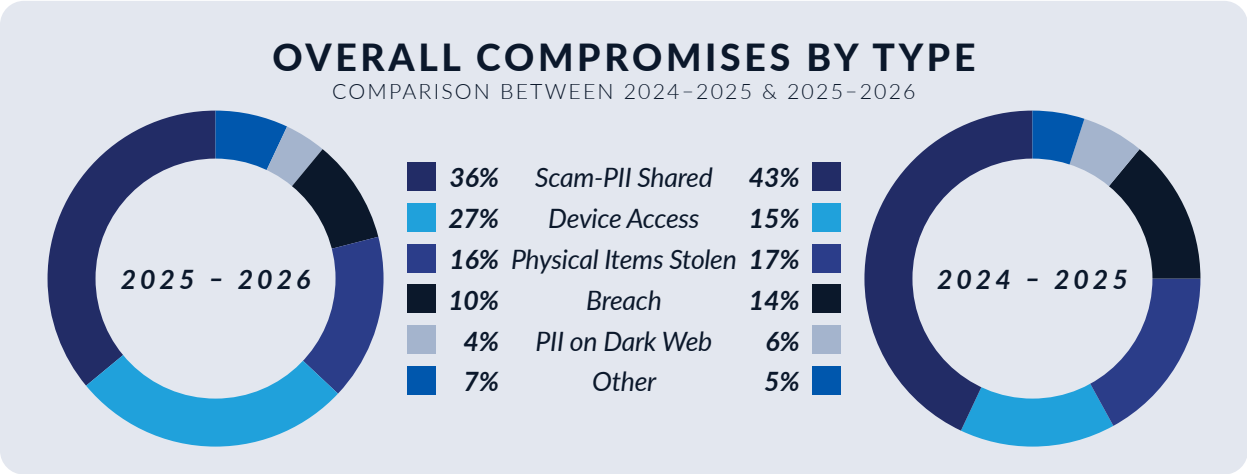
The next most common is account takeover combined with new account fraud (158 individuals), a pairing that reflects how these two crimes feed each other. In many cases, the takeover of an email account, phone carrier or credit reporting account gives a criminal the ability to intercept the verification alerts that would otherwise flag a fraudulent new account application.

The individuals who contact the ITRC with multiple incidents aren't simply unlucky. They are navigating a compounding crisis in which each new incident makes the next more likely and recovery more difficult.

TREND 2 *Device Access Has Overtaken Scams as the Primary Compromise for Working-Age Adults*

For the first time in the ITRC's reporting history, unauthorized access to a computer or mobile device has surpassed scams as the leading compromise method for adults between the ages of 35 and 64.

Overall, device access now accounts for 27.2 percent (27.2%) of all identity compromises reported to the ITRC – a 78 percent (78%) increase from the prior year, when it accounted for 15.3 percent (15.3%) of all compromises. Over the same period, scams involving the sharing of personal information declined from 43.1 percent (43.1%) to 36.1 percent (36.1%) of compromises. This shift is notable because the two compromise types work very differently.



A scam requires the victim's participation: a conversation, a moment of trust, a decision to share information. Device access does not. When our advisors speak with individuals who report this type of compromise, they most often describe their device as having been "hacked" – but in many cases, they can't tell us exactly how or when someone gained access. Unlike a scam, where the victim can usually walk us through the interaction that led to the compromise, device access often happens without the victim's knowledge. By the time they realize it, the damage has already spread.

When someone gains unauthorized access to a phone or computer, they can reach every account the victim is logged into – banking, email, social media, payment apps – without the victim being aware it's happening. The demographic pattern adds another layer. For adults aged 35-49, device access was the compromise method in 34 percent (34%) of cases. For adults 50-64, it was 38 percent (38%). These are working-age adults whose professional and personal lives are managed through their devices – and the compromise of a single device provides access to that entire ecosystem.

This trend has particular implications for survivors of domestic violence (also referred to as intimate partner violence). Among individuals who self-identified as domestic violence survivors and reported a compromise, 53 percent (53%) experienced unauthorized device access – nearly double the overall rate. Unlike other victims, domestic violence survivors can often identify the source: the person who accessed their device is someone they know. Our advisors hear this regularly – an abuser doesn't need to deceive someone they live with or have lived with. They already have access.

TREND 3 *The Recovery System Fails Victims Who Suffer Financial Harm*

The ITRC hears from individuals at every stage of the identity crime experience – from the person who just realized something is wrong to the person who has been navigating the aftermath for months. For the past several years, the ITRC has collected feedback from victims on the financial and emotional impacts of their experiences. This year, for the first time, we conducted a comprehensive analysis of that data for this report. What we found confirms what our advisors have long observed:

> *The system works reasonably well for people whose identity crime was caught early and caused limited damage.*
> **FOR EVERYONE ELSE, IT FALLS SHORT.**

Among the 147 victims who completed our financial impact survey, those who experienced crimes involving their personal information were typically managing three to four cascading financial consequences at once, including an inability to pay regular bills, depleted savings, reliance on public assistance and going without necessities. Scam victims face a different but equally serious financial reality. While our survey measures ongoing financial disruption rather than direct financial loss, our advisors work with scam victims every day whose savings have been depleted with no path to recover them, particularly older adults who may not have the ability to rebuild what was taken.

The most troubling finding is what happens when victims seek resolution. Among those with no measurable financial impact, 53 percent (53%) reported that their concern was ultimately resolved. Among those with any financial impact, that number drops to nine percent (9%). Among those who experienced three or more financial impacts, no one – zero percent (0%) – reported a resolution. While our survey sample is small (147 respondents), the pattern is consistent with what our advisors observe across thousands of interactions.

When an individual contacts the ITRC, they receive a recovery plan tailored to their specific circumstances. Our advisors walk alongside victims through a process that can take weeks or months, providing clarity in a system that often feels impossible to navigate.

TIR

IDENTITY THEFT RESOURCE CENTER

2026 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 4/1/25 – 3/31/26.*

ITRC | IDENTITY THEFT RESOURCE CENTER

CRIMES PER VICTIM

- ***74.4%*** *One (1) Incident*
- ***13.6%*** *Two (2) Incidents*
- ***5.9%*** *Three (3) Incidents*
- ***6.1%*** *Four (4) or More Incidents*

*Identity crimes have evolved from isolated events to "multi-layered" crises, with a **2.1 percentage-point increase** from the* PREVIOUS REPORTING PERIOD

***Unauthorized device access** **increased by 11.9 percentage points** from the previous reporting period.*

*Over the same period, **scams involving shared personal information declined by 7 percentage points**.*

REASONS WHY INDIVIDUALS CONTACTED THE ITRC

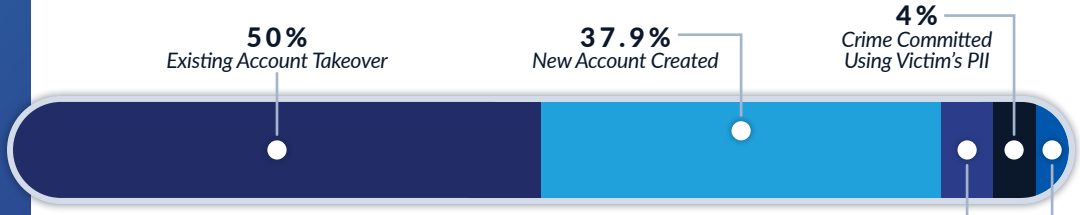
- **54.25%** *MISUSE CASES*
- **30.29%** *COMPROMISE CASES*
- **3.43%** *ATTEMPTED MISUSE*
- **12.03%** *PREVENTATIVE INFORMATION*

COMPROMISE BY TYPE

- *Scam Where PII Was Shared* ***36.1%***
- *Unauthorized Device Access* ***27.2%***
- *Physical Item(s) Stolen* ***16.4%***
- *Breach* ***10.2%***
- *PII on Dark Web* ***3.7%***
- *Other* ***6.4%***

*For the first time, **unauthorized device access** **surpassed scams** as the primary threat for* ADULTS AGED 35–64

IDENTITY MISUSE BY TYPE



***Fraudulent employment** is now the most common crime against minors, accounting for **40% of misuse cases** for* CHILDREN & DEPENDENTS

RECOVERY RATES

BASED ON REPORTED FINANCIAL LOSSES

*Among those who experienced three or more financial impacts, **zero (0) percent reported having reached a resolution.***

VICTIMS **WITH NO** FINANCIAL LOSS

Reported Being Able to Reach a Resolution

VICTIMS **WITH** FINANCIAL LOSS

Reported Being Able to Reach a Resolution

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.***

How Information Gets **EXPOSED**

How Information was Compromised

The Scam Experience

How Information Gets **EXPOSED**

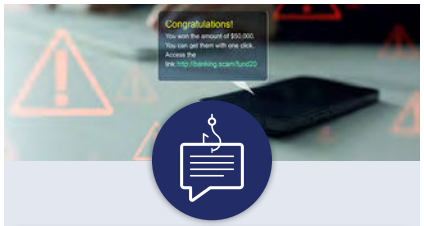
Before identity information can be misused, it must first be compromised. The individuals who contact the ITRC report a range of ways their personal information was initially exposed, from scams and device intrusions to stolen documents and data breaches. Understanding these entry points is critical to understanding everything that follows in this report:

> *The* **TYPE OF COMPROMISE** *shapes the* ***type of misuse****, the* ***severity of the impact*** *and the* ***path to recovery****.*

This year, 2,803 cases involved identity compromise, representing 30.3 percent (30.3%) of all cases reported to the ITRC.

How Information was **COMPROMISED**

Five primary compromise methods account for the vast majority of cases reported to the ITRC. The distribution shifted meaningfully from the prior year.



SCAMS
Victim Personal Information Shared

36.1% OF ALL CASES
Declined 7 Percentage Points from the Prior Year (43.1%)

UNAUTHORIZED DEVICE ACCESS

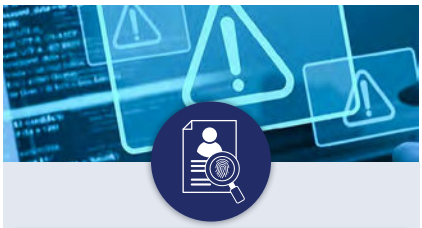
27.2% OF ALL CASES
Increased 11.9 Percentage Points from the Prior Year (15.3%)

PHYSICAL ITEMS STOLEN

16.4% OF ALL CASES
Remained Roughly the Same from the Prior Year

DATA BREACHES

10.2% OF ALL CASES
Declined 4.1 Percentage Points from the Prior Year (14.3%)



PII ON DARK WEB
Personally Identifiable Information

3.7% OF ALL CASES
Declined 2.3 Percentage Points from the Prior Year (6%)

The growth in physical items stolen warrants a note on our data. In the prior reporting period, the "Physical Items Lost/Stolen" category combined lost and stolen items. This year, we separated the two: stolen items are captured as compromises, while lost items are captured under preventative information requests. As a result, year-over-year comparisons for this category should be interpreted with that reclassification in mind.

Among individuals who reported stolen items, the most commonly reported were driver's licenses and state IDs (23.2%), Social Security cards (19.7%), credit and payment cards (11.8%) and birth certificates (10.3%). Phones and tablets accounted for just over seven percent (7.1%). These are the documents that form the building blocks of identity. As we discuss in *Section II*, the type of document stolen strongly predicts the type of misuse that follows.

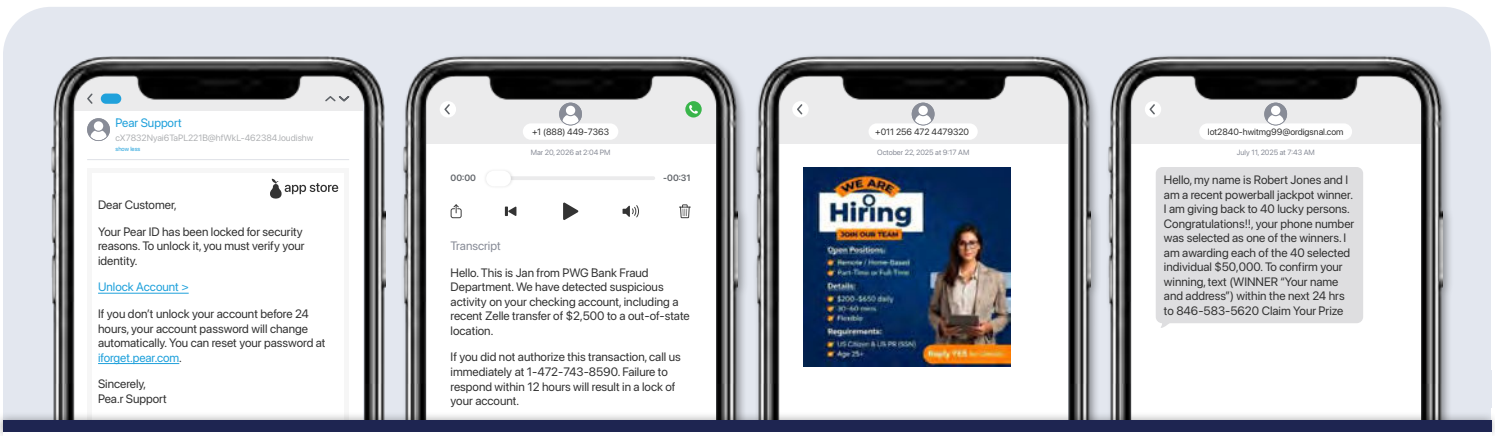
The SCAM EXPERIENCE

> **SOME OF THE MOST IMPACTFUL CONVERSATIONS I HAVE DAILY REVOLVE AROUND SCAMS.** *Some victims want tangible steps to take; others want someone to listen and offer reassurance. It brings me great pride to provide the tools victims need, in whatever capacity that may be.*
>
> *– Andy Llanes, Identity Theft Advisor*

While scam-related compromises declined as a share of total cases, scams remain the single most common way that personal information is exposed by a person. More importantly, the 1,286 scam cases reported this year reveal that not all scams operate the same way. Each scam type has a distinct profile: *who the scammer pretends to be, what information they extract and how often they succeed.*

HOW SCAMMERS OPERATE

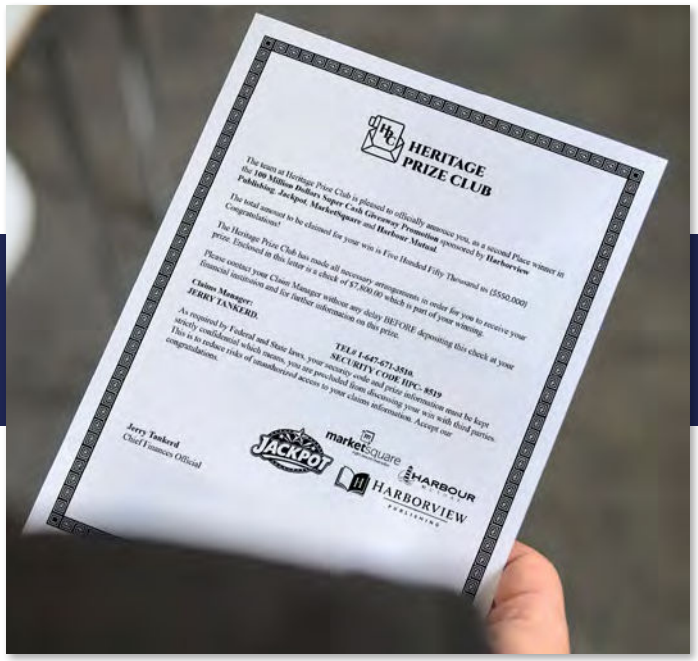
The most frequently reported scam type was ***"problems with the account"*** (26.4 percent (26.4%) of scam cases), in which a scammer contacts the victim claiming there is suspicious activity or a security issue with an existing account. This scam type saw significant growth from the prior year, though a portion of that increase reflects a change in how our team categorizes scams. In previous reporting periods, many of these cases would have been classified under the broader "impersonation" category. Beginning this reporting period, our advisors classify scams by the specific pretext used rather than the general tactic, providing a more detailed picture of how scammers operate.

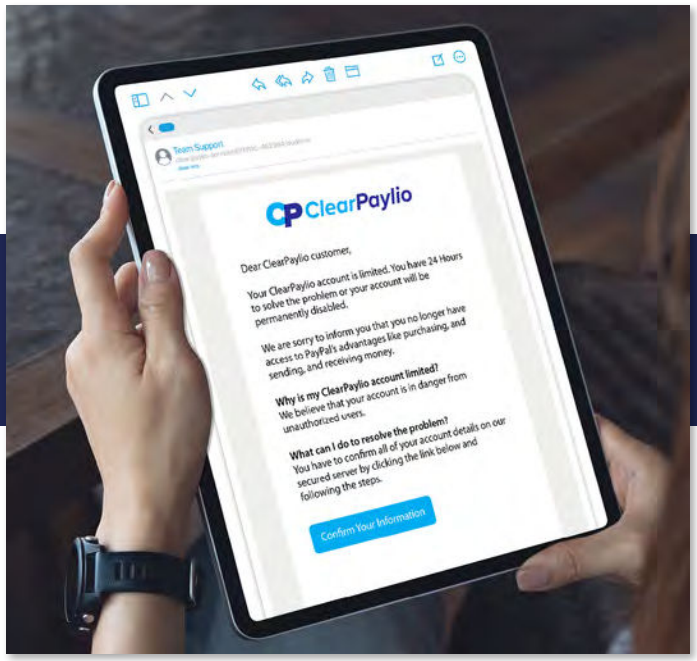


Account-problems scams are the highest-volume scam type, but what sets them apart is the quality of the information extracted: 74 percent (74%) of victims shared high-value PII, the highest rate of any scam category. When a scammer convincingly impersonates a bank or service provider, victims are more likely to hand over sensitive information such as Social Security numbers (SSNs), account numbers and payment card details, which enables the most damaging forms of misuse.

Job and employment scams were the second most common (11.4%) and the most intensive in terms of information harvested. Victims of job scams shared an average of four types of personal information per incident, the highest of any scam category. The PII profile reads like a job application weaponized: name (84%), address (54%), date of birth (52%), SSN (49%) and driver's license (46%). These scammers are trying to build complete identity packages.

Lottery and prize scams (7.5%) represent the opposite approach. Victims shared an average of just two types of PII, primarily their names and phone numbers. Only 25 percent (25%) shared any high-value PII such as a SSN or driver's license. These scams cast a wide net and extract relatively little identity information per victim, relying on volume and upfront "fees" rather than identity theft.



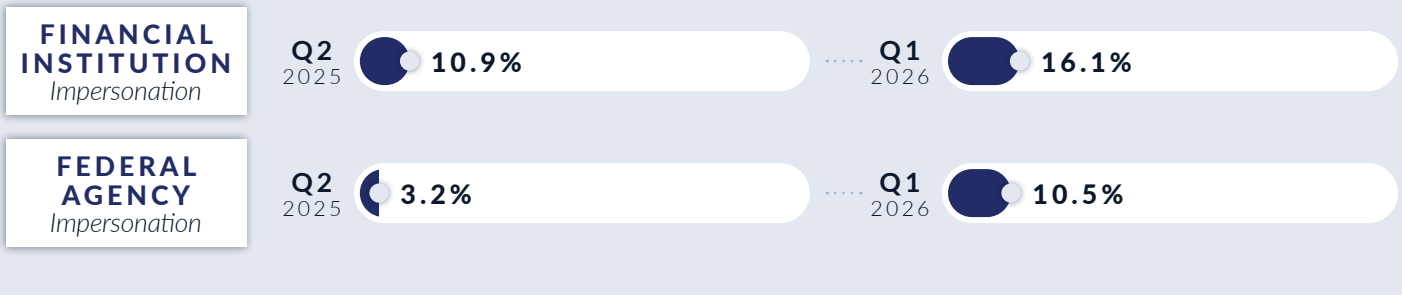


WHO SCAMMERS PRETEND TO BE

Among the 1,144 scam cases where the impersonation target was identified, nearly half (49.1%) involved scammers impersonating a business. Financial institutions accounted for 14.2 percent (14.2%), followed by potential employers or job recruiters at 9.1 percent (9.1%) and government agencies (federal, state or both combined) at 11.4 percent (11.4%).

The companies most frequently impersonated include PayPal (39 cases), American Express (35), Amazon (31), Publishers Clearing House (28), Dish Network (27), Microsoft (25), the Department of Homeland Security (DHS) (21) and the Social Security Administration (20). These concentrations suggest that certain brand names carry specific psychological weight depending on the scam type. Publishers Clearing House is almost exclusively associated with lottery and prize scams, appearing in 68 percent (68%) of cases with agency data. Microsoft accounted for 40 percent (40%) of tech support scams. DHS was the primary impersonation target in arrest and warrant scams.

Our quarterly data shows financial institution impersonation rising steadily over the reporting period, from 10.9 percent (10.9%) in Q2 2025 to 16.1 percent (16.1%) in Q1 2026. Federal agency impersonation also increased, from just over three percent (3.2%) to over ten percent (10.5%), with much of that growth concentrated in Q1 2026 (which coincides with tax season). These are patterns we are watching closely.



Our data categorizes each scam by its initial pretext, but our advisors hear a more complex story. Victims regularly describe scams that shift tactics during a single interaction. A call that begins as an account issue escalates into a law enforcement investigation. A romance develops into an investment opportunity. The victim experienced one continuous event, but the scam changed shape along the way. The ITRC continues to refine how we capture scam data, and reflecting these evolving tactics is a priority.

WHEN VICTIMS RECOGNIZE THE SCAM

Not every scam succeeds. Across all scam types, 21 percent (21%) of victims recognized the scam and did not share personal information. However, the rate varies dramatically by scam type.

Invoice scams had the highest recognition rate: 64 percent (64%) of victims did not share PII. These scams, which typically arrive as unexpected billing notices, tend to trigger immediate skepticism. Lottery and prize scams were recognized 42 percent (42%) of the time.

On the other hand, investment scams succeeded in extracting information 94 percent (94%) of the time. Job scams succeeded 92 percent (92%) of the time, and tech support scams 91 percent (91%). These are high-engagement scams that build trust through sustained interaction, making it harder for the victim to disengage once the relationship is established.

This range matters because it tells us something about where consumer education and awareness efforts can have the most impact. The scams with the highest recognition rates tend to be transactional and brief. The scams with the lowest recognition rates involve longer relationships and more emotional investment, which makes prevention fundamentally more difficult.

The ITRC was a resource I knew nothing about until the government shutdown. Thank God, literally, for this institution, given my circumstances. [ITRC Advisor] was my earth angel, my calm, patient, informative and, on top of it, guide all throughout this horrid experience of mine. [ITRC Advisor is] a face I won't see, a human I'll never forget. Thank you!

– ITRC VICTIM

I'm so thankful for the ID Theft Center because it's so much going around. Thanks [ITRC Advisor] for taking the time to explain and help me with the situation I was so worried about. I'm thankful [ITRC Advisor] was able to send me information because it is so much, and I want to make sure I do everything right.

– ITRC VICTIM

When Compromise Becomes **MISUSE**

How Compromise Channels into Misuse

What Was Stolen & What It Enabled

How Scam Type Shapes the Outcome

Attempted Misuse: When Defenses Catch Identity Thieves

When Compromise Becomes **MISUSE**

For most people who contact the ITRC, their experience falls into one of two categories: either their information was ***compromised*** or ***misused***. However, for 395 individuals during this reporting period, the experience didn't stop at exposure. Their compromised information was subsequently used against them, and we were able to trace the connection between how it happened and what followed.

This analysis, new for the 2026 report, examines those 395 individuals to understand the pathways from compromise to misuse. What we found is that the type of compromise doesn't just precede the type of misuse. It predicts it.

How Compromise CHANNELS INTO MISUSE

Among the 157 individuals whose devices were accessed without authorization and who subsequently experienced misuse, 87 percent (87%) experienced account takeover. This is the highest conversion rate of any compromise type, and it reflects the nature of the access: a compromised device gives a criminal direct entry into whatever accounts the victim is logged into. The criminal doesn't need a password or any additional information. They already have access to everything on the device.

Data breaches produced a distinctly different pattern. Among 48 individuals whose information was exposed through a breach and who experienced subsequent misuse, 62 percent (62%) experienced new account fraud, the highest rate of any compromise type, and 52 percent (52%) experienced account takeover.

UNAUTHORIZED ACCESS TO DEVICE

Existing Account Takeover

87%

DATA BREACHES

New Account Fraud

62%

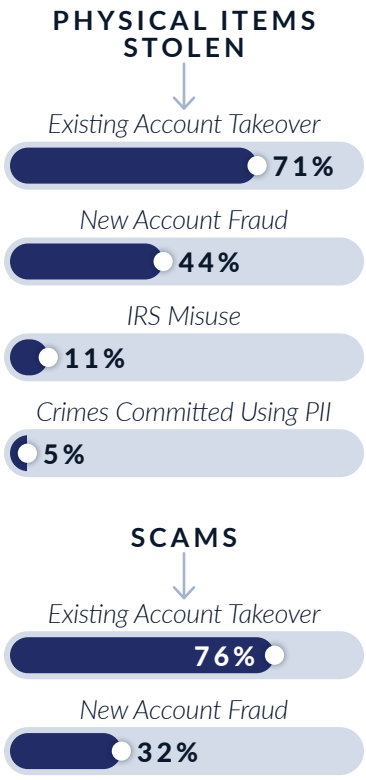
Existing Account Takeover

52%

Breaches often expose both login credentials and comprehensive personal information (name, SSN, date of birth, address), giving criminals the tools to pursue both paths. What sets breaches apart is that the breadth of information exposed in a single event provides everything needed to open new accounts, not just access existing ones.

Physical items stolen led to the broadest misuse profile. Among 94 individuals, 71 percent (71%) experienced account takeover, 44 percent (44%) experienced new account fraud, 11 percent (11%) experienced Internal Revenue Service (IRS) misuse and five percent (5%) experienced crimes committed using their PII. This is the only compromise type that produced meaningful rates of criminal identity theft, likely because stolen physical documents (driver's licenses, Social Security cards) can be used for impersonation in ways that digital data cannot.

Scam victims who experienced subsequent misuse (68 individuals) saw account takeover at 76 percent (76%) and new account fraud at 32 percent (32%). The scam provided the credentials or personal information the criminal needed to access or create accounts, but unlike device access, the criminal only obtained what the victim shared during the interaction.



What Was **STOLEN** *& What It* **ENABLED**

Among victims whose physical items were stolen, the specific item taken shaped the misuse that followed.

Stolen phones and tablets led to account takeover in 100 percent (100%) of cases (14 individuals). A phone contains active sessions for banking, email, social media and payment apps, giving a criminal immediate access to existing accounts. This finding underscores that device security is just as important as account security. A strong password on a payment app matters less if the phone that stays logged into that account has no screen lock, no remote wipe capability and no multi-factor authentication (MFA).

Stolen mail channeled primarily into new account fraud (80 percent (80%) of five individuals), consistent with intercepted financial documents being used to open accounts. Stolen driver's licenses produced the widest range of downstream misuse, including account takeover (86%), new account fraud (57%) and IRS misuse (43%), reflecting that a government-issued ID enables both financial fraud and impersonation in government systems.

We present these item-level findings with a caveat: *the individual counts are small, and the patterns should be understood as directional rather than definitive. What they consistently show is that the type of document or item stolen is not random in its consequences. Each item opens a specific set of possibilities for the criminal.*

How Scam Type **SHAPES THE OUTCOME**

Among the 68 scam victims who experienced subsequent misuse, the type of scam influenced what happened next.

Account-Problems Scams
Account-problems scams were heavily channeled into account takeover at 84 percent (84%) (32 individuals with misuse of data). This is consistent with the nature of the scam: the victim, believing they are resolving an issue with an existing account, provides the exact credentials needed to access that account.

Romance Scams
Romance scams produced the broadest misuse spread of any scam type. Among the small number of romance scam victims in this analysis (eight individuals with misuse data), 62 percent (62%) experienced account takeover, 50 percent (50%) experienced new account fraud and 25 percent (25%) experienced IRS misuse. The extended trust-building of a romance scam means victims often share comprehensive personal information over time, giving the criminal enough data to pursue multiple types of misuse simultaneously.

Job & Employment Scams

Job and employment scams led to account takeover in 88 percent (88%) of cases (eight individuals with misuse of data). The account types taken over reflect the onboarding pretext: identity verification accounts like ID.me and bank accounts provided for 'direct deposit' were the most common targets. Despite being the scam type that harvests the most PII overall, the downstream misuse is concentrated in accounts that mirror what a legitimate employer would request.

"My identity has been stolen four times within the past six months, and I've had to freeze my debit accounts and two of my credit cards! My mail is going everywhere but into my mailbox, and I've lived at the same address for 30 years now."

– ITRC VICTIM

"I appreciate your concern and moral support. It's been a really frustrating and time-consuming experience, and I've been dealing with this at the same time as a relative was deported and I was hospitalized. No one needs this BS in their life."

– ITRC VICTIM

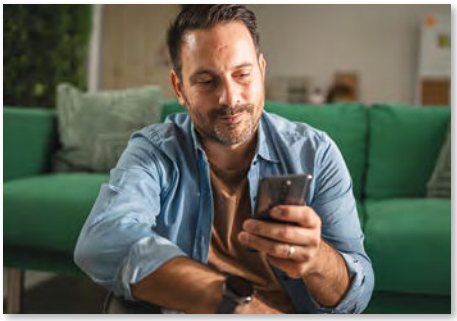
ATTEMPTED MISUSE: *When Defenses Catch Identity Thieves*

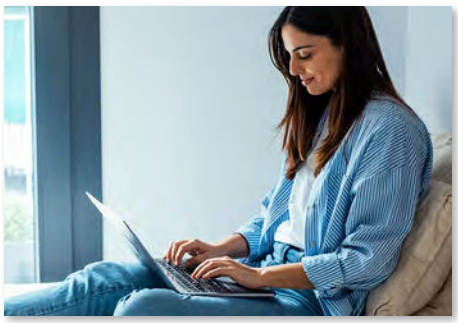
Not every compromise leads to successful misuse. During this reporting period, 317 cases involved attempted misuse that was caught before completing, a 26.8 percent (26.8%) increase from the prior year.

Of the attempted misuse cases, 62.1 percent (62.1%) involved new account applications, and 37.9 percent (37.9%) involved attempted account takeovers. Credit cards accounted for 41 percent (41%) of all attempted misuse by account type, followed by checking accounts at 17.7 percent (17.7%) and personal loans at 8.5 percent (8.5%).

How these attempts were caught is significant. Two-thirds (67%) were discovered through account issuer notifications. The victim's financial institution detected the fraud before the victim did. Credit and identity theft monitoring caught another five percent (5%), and credit report checks caught eight percent (8%).

This data points to something worth acknowledging: institutional fraud detection systems are working. They are catching a meaningful volume of fraudulent activity before it results in a completed crime. However, the protection is concentrated in financial accounts with mature detection infrastructure. Attempted employment fraud, IRS misuse and criminal identity theft rarely appear in this data because there are fewer automated systems designed to catch them before they succeed. The crimes that are hardest to detect are also the hardest to prevent, and as we discuss in *Section III*, they are often the hardest to resolve.





Identity Misuse:

What Criminals Do With **STOLEN** *Information*

Account Takeover

New Account Fraud

The Crimes That Are Hardest to See

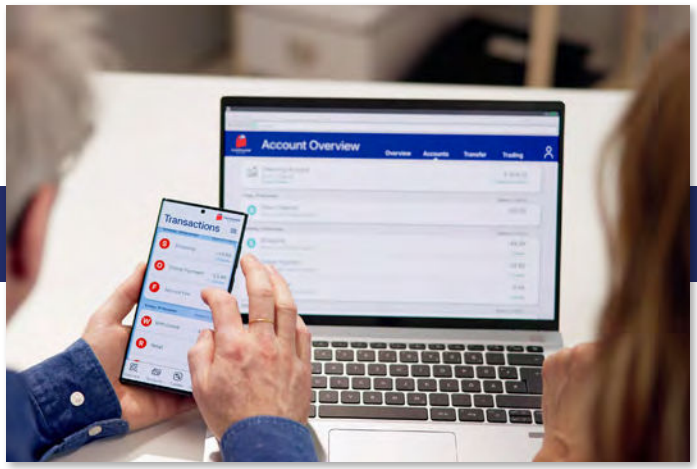
What Criminals Do With **STOLEN** *Information*

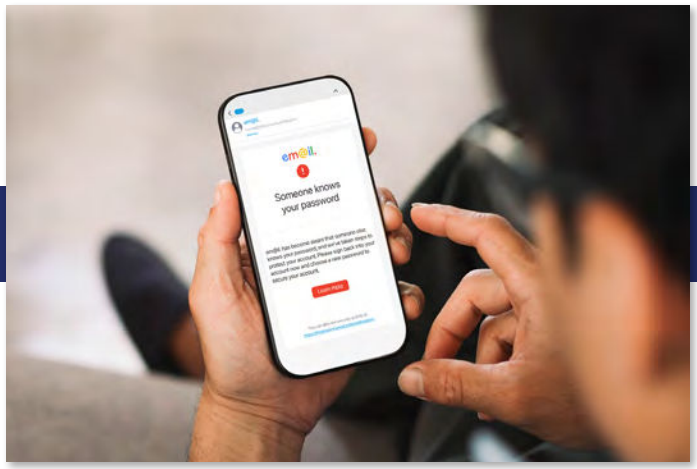
Once personal information has been compromised, the question becomes how it is used. Misuse accounted for 54.3 percent (54.3%) of all cases reported to the ITRC this year (5,020 cases), up from 51.8 percent (51.8%) the prior year. Two categories account for the vast majority: existing account takeover and new account fraud. With that said, the smaller categories (fraudulent employment, IRS misuse and criminal identity theft) are often the ones that cause the most lasting harm and are the hardest for victims to discover and resolve.

Account **TAKEOVER**

Account takeover remains the most common form of identity misuse, accounting for 50 percent (50%) of all misuse cases (2,512 cases). When a criminal gains control of an existing account, the victim typically learns about it quickly because they either notice unauthorized activity or lose access entirely.

> *That visibility, while distressing, often means the victim can* **BEGIN ADDRESSING THE PROBLEM SOONER**.





The most frequently targeted account types were checking accounts (25.3%), credit cards (18.7%) and email (13.5%). Cell phone carriers accounted for just over five percent (5.3%), followed by peer-to-peer (P2P) payment apps (3.1%), personal tech accounts (2.7%), merchant accounts (2.7%) and credit reporting agencies (2.7%).

Checking Accounts	*Credit Cards*	*Email*
25.3%	**18.7%**	**13.5%**

How victims discover account takeover depends on the account type, and these patterns reveal something important about which accounts have built-in detection and which do not. When victims discovered account takeover by checking their own accounts (28 percent (28%) of cases), the top targets were checking accounts (38%) and credit cards (21%): financial accounts with visible transaction histories that people review regularly. When account takeover was discovered because the victim could no longer log in (20 percent (20%) of cases), email (34%) and social media (32%) led. These are accounts where the first sign of trouble is a lockout, not a suspicious charge. When the account issuer notified the victim (22 percent (22%) of cases), credit cards led at 36 percent (36%), reflecting the strength of financial institutions' fraud detection systems.

DISCOVERY METHODS OF ACCOUNT TAKEOVER

For individuals dealing with multiple identity incidents, the account takeover account profile expands. Among multi-incident individuals, email rises from nine percent (9%) to 16 percent (16%) of account takeover cases, cell phone carrier from three percent (3%) to six percent (6%) and personal tech accounts from two percent (2%) to four percent (4%), while credit cards' share declines from 25 percent (25%) to 16 percent (16%). This shift reflects criminals working through a victim's broader digital ecosystem rather than targeting a single financial account. Taking over an email or phone carrier account allows resetting passwords and intercepting verification codes across multiple other accounts.

Our quarterly data shows this expansion in real time. Cell phone carrier account takeovers rose from just under four percent (3.9%) of account takeover cases in Q2 2025 to just under seven percent (6.8%) in Q1 2026. Merchant account takeovers tripled from one and a half percent (1.4%) to four and a half percent (4.4%) over the same period. These emerging targets are worth watching as they may indicate that criminals are adapting to stronger protections on traditional financial accounts by shifting to accounts with less mature fraud detection.

New Account **FRAUD**

New account fraud was the second-most-common form of misuse, accounting for 37.9 percent (37.9%) (1,905 cases).

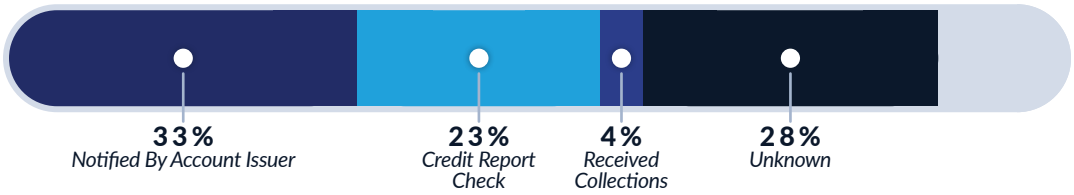
Unlike account takeover, new account fraud is largely
INVISIBLE TO THE VICTIM.

Someone opens a credit card, takes out a loan or signs a lease using the victim's information, and the victim has no way of knowing until the consequences surface.

Credit cards were the most common fraudulent account type at 32.7 percent (32.7%), followed by checking (9.5%), personal loans (8.0%), cell phone carriers (5.4%), auto loans (5.1%) and mortgage loans (4.5%). Federal student loans accounted for just under three percent (2.8%).

The way victims discover new account fraud is fundamentally different from how they discover account takeover. The primary detection method was notification from the account issuer (33%), often a financial institution alerting the victim that an account was opened, or an application was submitted in their name. Credit report checks accounted for 23 percent (23%) of discoveries. Collections notices, where the victim learns about a fraudulent account only when it goes unpaid and reaches collections, accounted for four percent (4%). These are slower, more passive discovery mechanisms, which means some victims don't find out about fraudulent accounts for weeks or months.

DISCOVERY METHODS OF NEW ACCOUNT FRAUD



This has a practical implication: regularly checking your credit report is the single most effective way to detect new financial account fraud. Twenty-three percent (23%) of all new account fraud cases in our data were discovered this way. Credit freezes, which prevent new accounts from being opened without the consumer's explicit authorization, remain the strongest preventative measure.

Among multi-incident individuals, the new account creation account profile shifts toward higher-value and longer-term fraud. Auto loans rose from three percent (3%) (single incident) to seven percent (7%) (multi-incident), mortgage loans from four percent (4%) to five percent (5%) and property leases from one percent (1%) to three percent (3%). These are not quick credit card applications. They represent criminals building fraudulent financial lives using the victim's identity.

Our quarterly data shows several new account creation account types accelerating. DMV-related accounts rose from just under one percent (0.7%) to three percent (3%) of new account creation cases over the reporting period, suggesting criminals are obtaining fraudulent driver's licenses as foundation documents for further fraud. Federal student loans increased from just under two percent (1.8%) to just over four percent (4.2%). Point-of-sale finance accounts (buy-now-pay-later products) emerged from nearly zero to two-point-three percent (2.3%) of new account creation cases, concentrated almost entirely in Q1 2026. These newer financial products may have identity verification processes that have not yet kept pace with the sophistication of the fraud targeting them.

The Crimes That Are **HARDEST TO SEE**

Fraudulent employment, IRS misuse and criminal identity theft together account for 12 percent (12%) of all misuse cases. Their combined volume is modest compared to account takeover and new account fraud.

These are the crimes that most fundamentally disrupt a person's life, and they share a common characteristic: **VICTIMS ALMOST NEVER DISCOVER THEM ON THEIR OWN.**

"They were straight to the point and knew exactly what I needed. I feel a lot better about my situation and confident that someone is in my corner to help me through this."

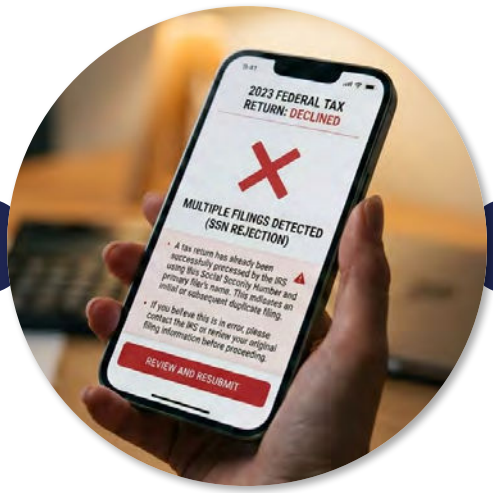
– ITRC VICTIM

"The company refused to move forward to help resolve the issue, even after sending them a dispute letter of identity theft, along with an FTC report and police report."

– ITRC VICTIM

FRAUDULENT EMPLOYMENT – *244 Cases, 4.9% of Misuse*
Occurs when someone uses a victim's identity to gain employment. The victim typically has no idea until something goes wrong. Twenty-three percent (23%) discovered the fraud while applying for government benefits and learning that benefits had already been claimed or that income had been reported under their SSN. Nineteen percent (19%) were notified by a government agency. Thirteen percent (13%) were denied benefits outright. Six percent (6%) learned about it through a fraudulent 1099 tax form.

This crime has a disproportionate impact on children. Among child and dependent victims in our data, fraudulent employment accounted for 40 percent (40%) of all misuse cases, making it the most common crime against minors by a wide margin. Children's SSNs are valuable to criminals precisely because they are clean: most parents and guardians are not looking for a child's existing credit history or employment record, which would trigger a conflict. A child's identity can be used for years before anyone notices.



IRS MISUSE – *159 Cases, 3.2% of Misuse*
Primarily involves someone filing a tax return using the victim's information. This accounted for 85.4 percent (85.4%) of IRS misuse cases. Victims most commonly found out through government notification (61%), whether from the IRS directly or another government agency. Seven percent (7%) discovered it while checking their own accounts, often when an expected refund did not arrive or had already been issued to an account they didn't recognize.

CRIMINAL IDENTITY THEFT – *200 Cases, 4% of Misuse*
Is the most severe and the most difficult to resolve. Someone uses the victim's identity during an interaction with law enforcement, creating a criminal record in the victim's name. Discovery almost always comes as a shock: 34 percent (34%) learned about it from law enforcement, often during a traffic stop or other routine encounter. Fourteen percent (14%) discovered it through a background check, frequently during a job application process. Six percent (6%) learned about it from an employer.

What connects these three crime types is that the victim has no direct line of sight into the system where the misuse is occurring. There is no account statement to review, no login to check, no balance to monitor. While the IRS does notify some victims of suspicious activity, these notifications are not as consistent or timely as the fraud alerts that financial institutions provide. The employment verification and criminal justice systems have even fewer mechanisms for proactive notification. By the time these crimes surface, the damage is often well established, and untangling it requires navigating government agencies, employers and law enforcement over a process that can take months or years.

Who Is Affected:

DEMOGRAPHICS & VULNERABLE POPULATIONS

Identity Crime By Age

Household Income

Children & Dependents

When the Thief is Someone You Know

Vulnerable Populations

DEMOGRAPHICS & VULNERABLE POPULATIONS

Identity crimes do not affect everyone the same way. The type of crime a person experiences, how their information was compromised and the likelihood of facing multiple incidents all vary by age, gender and life circumstances. This section examines those patterns because understanding who is targeted and how is essential to building effective prevention and response strategies.

Identity Crime **BY AGE**

> *In my experience supporting victims of identity theft, especially the elderly, I've learned that recovery is not just a technical process;* **IT IS A JOURNEY THAT REQUIRES PATIENCE, TRUST AND COMPASSION.**
>
> *– Cindy Morales, Director of Victim Services*

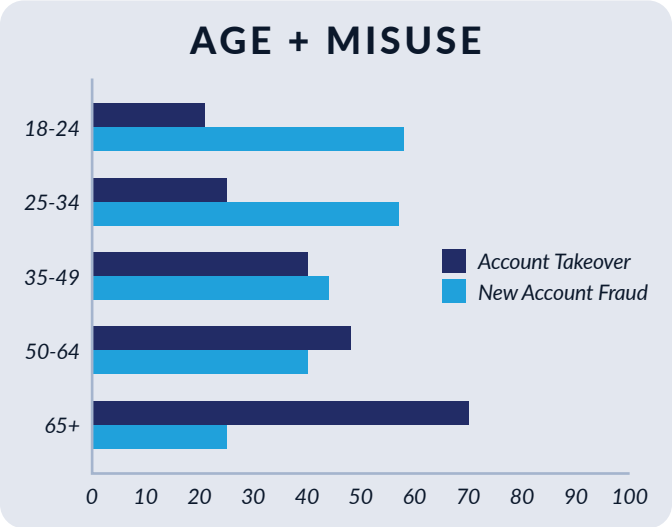
The relationship between age and identity crime type is one of the most consistent patterns in our data. The misuse profile essentially inverts from youngest to oldest.

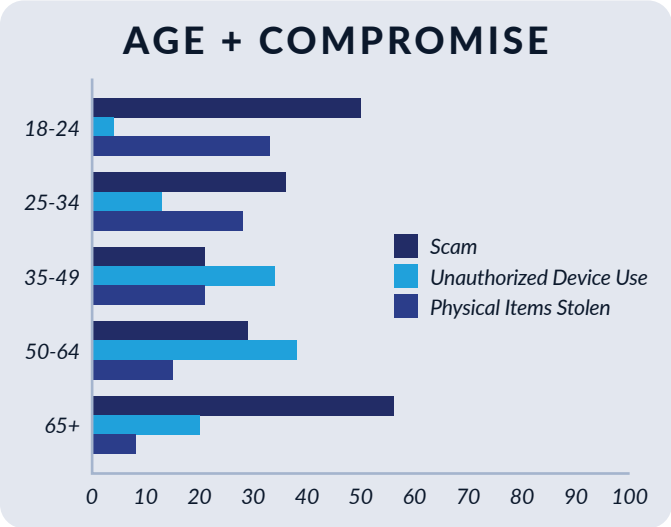
Among individuals aged 65 and older, account takeover accounted for 70 percent (70%) of misuse cases, with new account fraud at 25 percent (25%). For adults aged 18-24, the pattern reverses: new account fraud led at 58 percent (58%), with account takeover at just 21 percent (21%). The transition between these two endpoints is gradual and consistent across every age group. Account takeovers share rises from 15 percent (15%) for minors, to 21 percent (21%) for 18-24, to 25 percent (25%) for 25-34, to 40 percent (40%) for 35-49, to 48 percent (48%) for 50-64, to 70 percent (70%) for 65 and older.

This reflects a straightforward reality: older adults have more established financial accounts with higher balances, making those accounts more valuable targets for takeover. Younger adults have thinner credit histories, which makes new account fraud more productive because there are fewer existing records to trigger a conflict.

The compromise pathway also varies by age. Adults 65 and older were most likely to have their information compromised through a scam (56 percent (56%) of compromise cases), consistent with the sustained, trust-based scam types (romance, account-problems, tech support) that disproportionately target older adults. For adults aged 35-64, unauthorized device access was the leading compromise method (34 percent (34%) for ages 35-49, 38 percent (38%) for ages 50-64), a pattern we discuss in detail in *Trend 2*.

Younger adults aged 18-24 had the highest rate of physical items stolen at 33 percent (33%), reflecting the practical reality that phones, wallets and documents are more vulnerable to theft for people who are more mobile and may have less stable or secure living situations.





The multi-incident rate peaks among working-age adults. Adults aged 35-49 had the highest rate at 37 percent (37%), followed by 50-64 at 35 percent (35%) and 65 and older at 32 percent (32%). The lowest rates were among 18-24 (18%) and minors (7%). This pattern suggests that the complexity of identity crime increases with the complexity of a person's financial and digital footprint.

Household **INCOME**

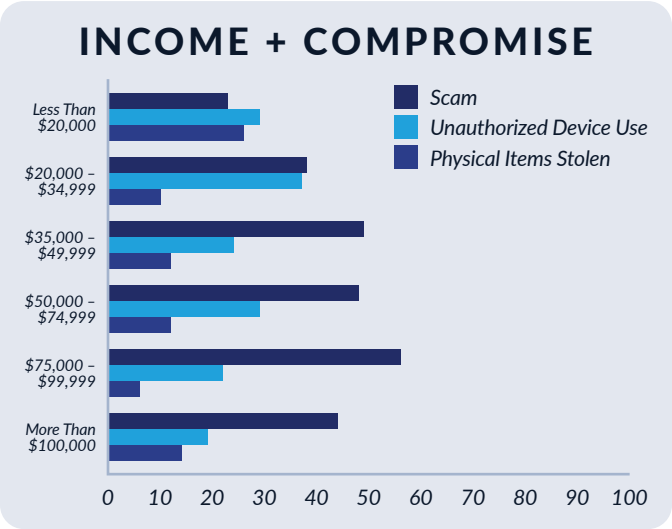
The ITRC collects household income on a voluntary basis using broad ranges. During this reporting period, 30 percent (30%) of individuals provided this information.

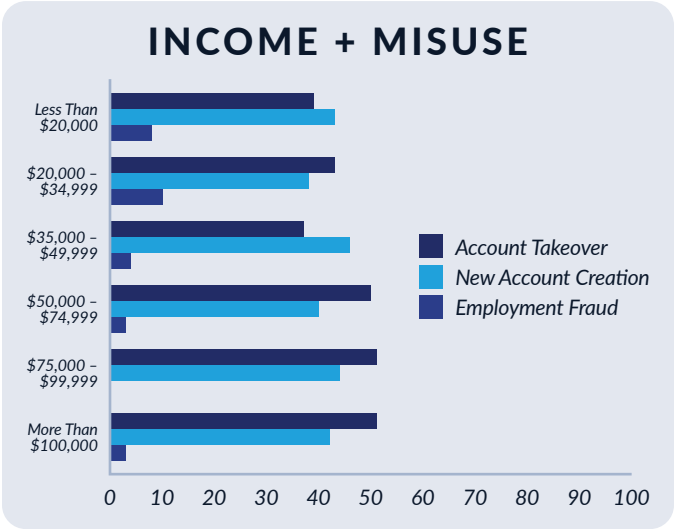
We note that income is one of the demographic fields that individuals are least comfortable sharing *and the findings below reflect only those who chose to do so.*

Even within that limitation, the data reveals a clear pattern: the type of identity crime a person experiences is shaped in part by their economic circumstances.

Among individuals with household incomes below $20,000, physical items stolen was the compromise method in 26 percent (26%) of cases, compared to six percent (6%) to 14 percent (14%) for higher income brackets. Scam-related compromise was lowest for this group at 23 percent (23%), compared to 44 percent (44%) to 56 percent (56%) for individuals earning $35,000 or more. The practical explanation is straightforward: individuals with fewer resources may have less ability to physically secure documents and devices, while higher-income individuals are more likely to be targeted through digital social engineering.

The misuse pattern follows a similar gradient. Lower-income individuals experienced higher rates of new account fraud (43%), fraudulent employment (8%) and crimes committed using their PII (5%). Higher-income individuals were more likely to experience account takeover (51 percent (51%) for those earning over $100,000, compared to 39 percent (39%) for those earning under $20,000). This mirrors the age-based pattern discussed above: account takeover targets established accounts with higher balances, while new account fraud and employment fraud target the identity itself.





Notably, the crime types that are more prevalent among lower-income individuals (new account fraud, fraudulent employment and crimes committed using their PII) are also the crime types identified in *Section III* as the hardest for victims to discover and, as discussed in *Trend 3*, the least likely to result in resolution. Lower-income individuals in our data are disproportionately facing the crimes that the current system is least equipped to detect and address.

Lower-income individuals also had the highest multi-incident rate at 37 percent (37%), compared to 27 percent (27%) to 33 percent (33%) for other income groups. This finding is consistent with the broader pattern in our data: individuals with fewer resources to secure their identity and respond to initial compromises are more likely to experience cascading incidents.

CHILDREN & DEPENDENTS

Identity crimes against children and dependents represented 247 cases involving 204 unique victims. As discussed in *Section III*, fraudulent employment is the most common crime against children, accounting for 40 percent (40%) of their misuse cases. However, the full picture of child identity crime extends beyond employment fraud.

In 83 percent (83%) of child cases, the alleged thief was unknown. When the thief was identified, ex-spouses and partners were the most common at six percent (6%), followed by a parent at three percent (3%). These known-thief cases often reflect family situations where a parent or former partner uses a child's SSN to open accounts or obtain employment, potentially out of financial desperation rather than malicious intent. Regardless of the reason, the impact can significantly impede that child's ability to secure financial or utility accounts. A child whose identity was used for fraudulent employment at age 5 may not discover the damage until they apply for their first student loan at 18 or a job at 16.

What makes child identity crime particularly challenging is the timeline. Since most parents and guardians do not monitor their child's credit, fraud can go undetected for years. By that point, untangling the history is significantly more complicated.

When the Thief is **SOMEONE YOU KNOW**

In 86 percent (86%) of cases reported to the ITRC, the alleged thief is unknown to the victim. However, among the 13 percent (13%) of individuals who could identify the person responsible, the relationship between the victim and the thief strongly predicts the type of crime.

Ex-Spouses & Partners – *218 Cases*
The most frequently identified thief. Their crime profile is defined by proximity and access: 52 percent (52%) of their misuse cases involved account takeover, and among those with a known compromise, 65 percent (65%) involved unauthorized device access. These are individuals who know passwords and security question answers, and who have historical access to shared accounts.

Parents as Thieves – *68 Cases*
Had the highest new account fraud rate at 67 percent (67%). This pattern is consistent with parents using a child's clean credit profile to open accounts, often for utilities, credit cards or loans. The parent has access to the child's SSN and personal information from birth.

Siblings as Thieves – *41 Cases*
Siblings as thieves (41 cases) produced the most distinctive pattern: 35 percent (35%) of their misuse cases involved crimes committed using the victim's PII, the highest rate of any thief relationship and nearly nine times the overall rate of four percent (4%) across all misuse cases. Our advisors hear from victims whose siblings used their identity documents during interactions with law enforcement, a form of impersonation that is more plausible when the individuals share a family resemblance and residence.

Traffickers – *24 Cases*
Produced the second-highest new account fraud rate at 65 percent (65%). This reflects the systematic exploitation of victims' identities under coercion. Trafficking survivors in our data experienced 62 percent (62%) new account fraud overall, and their compromise was overwhelmingly through device access (45%) or physical theft (20%), both reflecting the trafficker's direct physical control over the victim.

Neighbors **–** *36 Cases*
Had the highest account takeover rate of any thief relationship at 68 percent (68%), with device access accounting for 49 percent (49%) of their compromise cases. Proximity without the emotional complexity of a family relationship may make neighbors more likely to exploit access purely for financial gain.

These patterns matter for two reasons. First, they illustrate that identity crime committed by someone the victim knows looks fundamentally different from identity crime committed by a stranger. The compromise method, the misuse type and the emotional toll are all shaped by the relationship. Second, they highlight that victims who know their thief often face additional barriers to reporting and recovery, including fear of retaliation, family pressure to not pursue the matter and the emotional weight of accusing someone they have a personal relationship with.

VULNERABLE *Populations*

Certain populations face identity crime profiles shaped by the specific vulnerabilities of their circumstances. The ITRC collects targeted population data on a self-identified basis, and the findings below reflect those individuals who chose to share this information.



Domestic Violence Survivors **–** *139 Individuals*
Experienced the most distinctive compromise profile: 53 percent (53%) unauthorized device access, as discussed in *Trend 2*. On the misuse side, 60 percent (60%) experienced account takeover. Among domestic violence survivors who identified their thief, 54 percent (54%) named an ex-spouse or partner, and ten percent (10%) named a current spouse or partner. The identity crime is often an extension of the abuse itself.

Individuals Experiencing Homelessness **–** *53 Individuals*
Reported the highest rate of physical theft among any population at 53 percent (53%) of their compromise cases, compared to an overall rate of 16 percent (16%). Their misuse profile showed elevated rates of IRS misuse (eight percent (8%) vs. three percent (3%) overall) and crimes committed using PII (seven percent (7%) vs. four percent (4%)), consistent with stolen physical documents being used for government benefits fraud and impersonation.

Trafficking Survivors – *48 Individuals*
Experienced the highest new account fraud rate of any population, at 62 percent (62%) of misuse cases. Their information was compromised primarily through device access (45%) and physical theft (20%), both reflecting the coercive control that defines trafficking situations. The near-absence of scam-related compromise (5%) among trafficking survivors confirms that their data is taken through force, not deception.

Formerly Incarcerated Individuals – *55 Individuals*
Reported elevated new account fraud (54%) and the highest rate of crimes committed using PII (8%) among targeted populations. Their identities may be exploited during or after incarceration, when they have limited ability to monitor their credit or respond to misuse.

Individuals Who Are Deaf or Hearing Impaired – *27 Individuals*
Were the only targeted population where scam-related compromise led at 56 percent (56%), above the overall rate. They also reported the highest rates of both IRS misuse (12%) and criminal identity theft (12%) among targeted populations. Communication barriers may make it harder for these individuals to respond to identity misuse once it begins.

The ITRC recognizes that vulnerability to identity crime is a product of circumstances, systems and access. Our advisors are trained to meet every person where they are and to adapt our guidance to their specific situation, because recovery looks different for a trafficking survivor than it does for a retiree, even when the underlying crime is the same.

Additional demographic data, including gender and ethnicity breakdowns by crime type, are available in the *Appendix*.

"I would like to say that [ITRC Advisor] is outstanding. I suffer from panic and anxiety, and [ITRC Advisor] has been very kind and gentle and keeps calling to check up on me. I realize the process is very long. I'm running into roadblocks, but I speak to [ITRC Advisor] once a week, and she sends me in a different direction to try to resolve [the case]. Thank you, she's an asset to your company. And I am so grateful that I reached out and found her."

– ITRC VICTIM

The HUMAN IMPACT

Emotional Impact

Financial Impact

Working With the ITRC

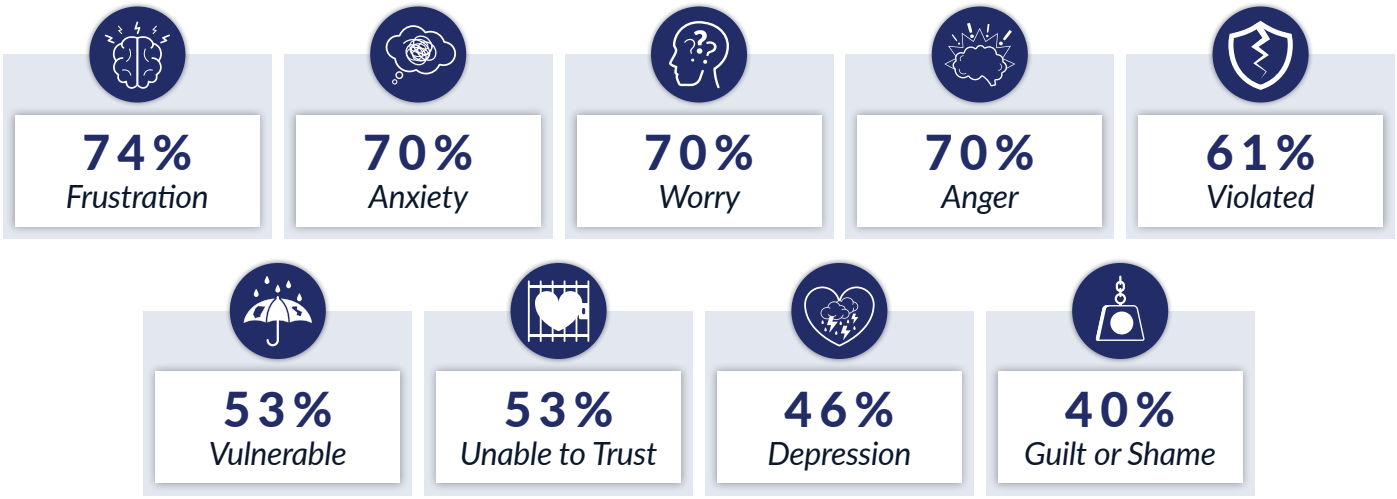
The HUMAN IMPACT

The data in this report describes crimes in categories and percentages. This section describes what those crimes feel like for the people experiencing them. For the past several years, the ITRC has collected feedback from victims through surveys on emotional and financial impact. This year, we analyzed that data alongside our satisfaction survey to understand not just what happened to individuals, but how it affected them and what helped.

The emotional impact survey reflects 261 respondents, the financial impact survey reflects 147 and the satisfaction survey reflects 236. These are individuals who chose to participate, and their experiences may not represent all identity crime victims. We present this data as a window into the human side of identity crime, grounded in what these individuals told us.

EMOTIONAL *Impact*

Among the 257 respondents who described their emotional experience, the average person reported six distinct emotional responses.



Each crime type produced a **DISTINCT EMOTIONAL PROFILE**.

Scam victims reported the highest rates of guilt and shame at 57 percent (57%), a reflection of the self-blame that often accompanies being deceived. Our advisors see this regularly: victims feel responsible for having been manipulated, even when the scam was sophisticated and deliberately designed to exploit trust. Account takeover victims reported the highest average number of emotional responses at seven per person, suggesting that the experience of losing control of an existing account produces a broad emotional reaction.

Victims of fraudulent employment and crimes committed using their PII reported the highest emotional intensity, averaging eight emotional responses per person. Depression rates for these crime types reached 89 percent (89%) and 57 percent (57%), respectively, well above the overall rate of 46 percent (46%). These are the crime types discussed in *Section III* as the hardest to detect and resolve, and the emotional data reflects that: crimes that take longer to discover and are more difficult to untangle produce deeper and more sustained emotional harm.

"I was having a nervous breakdown and couldn't get help from anybody until [ITRC Advisor] called me and did an extraordinary job of putting my mind at ease. I now feel like I can breathe. Thank you [ITRC Advisor]. You are amazing."

– ITRC VICTIM

Across all crime types, just under ten percent (9.7%) of respondents reported experiencing suicidal ideation as a result of their identity crime[1]. Among the small number of respondents who experienced crimes committed using their PII, that rate was 43 percent (43%). We share these findings because they reflect the reality that for some individuals, identity crime is not a financial problem. It is a crisis that affects their sense of safety, their mental health and their ability to function.

Only 32 percent (32%) of respondents sought emotional support. Those who did were less likely to have their concern resolved (20%) than those who did not seek support (40%). This suggests that the individuals whose situations were severe enough to seek emotional help were also facing more complex and difficult-to-resolve crimes.

FINANCIAL *Impact*

The financial consequences of identity crime extend well beyond the initial loss. Among the 147 individuals who completed our financial impact survey, 55 percent (55%) reported at least one ongoing financial consequence. The most common were debt (35%), inability to pay regular bills (31%), being denied credit or loans (29%), depleted savings (21%) and inability to pay rent (21%). Fifteen percent (15%) were denied a checking account. Four percent (4%) were forced to declare bankruptcy.

[1] The ITRC also reports the number of victims who considered self-harm in the annual *Consumer Impact Report* (CIR) published each October. The rate of victims experiencing suicidal ideation differs between the two reports based on the time period considered - three months for victim feedback in this report versus a response period that ranges from 1 to 12 months in the CIR – and the number of individuals responding to the questionnaires used to gather this information.

When asked how they managed financially, 36 percent (36%) said they went without necessities to make ends meet. Twenty percent (20%) borrowed money from friends or family. Seventeen percent (17%) relied on credit cards. Fourteen percent (14%) sought government assistance. Four percent (4%) obtained payday loans, adding new debt to their existing debt.

As discussed in *Trend 3*, the relationship between financial harm and resolution is stark. We see this pattern clearly in our data: the more financial consequences a victim faces, the less likely they are to reach a resolution[2]. Among those who reported no financial impact, 53 percent (53%) had their concern resolved. Among those with any financial impact, nine percent (9%) had their concern resolved. Among those with three or more, no concerns were resolved.

The individuals behind these numbers are people who contacted the ITRC looking for a path forward. Seventy-four percent (74%) had taken the steps outlined in their recovery plan. They were doing what was recommended. The gap between effort and outcome is not a reflection of the victim. It reflects systems that are not designed to address cascading financial harm.

Working With the **ITRC**

236 Individuals Completed Our Satisfaction Survey:

Satisfaction With **ADVISOR**

90% *Rated 4 or 5 Out of 5*

Advisor **DEDICATION**

88% *Rated 4 or 5 Out of 5*

Advisor's Expert **KNOWLEDGE**

89% *Rated "Knowledgeable"*

Comfort With Received **CASE PLAN**

83% *Rated "Comfortable"*

The quantitative scores tell part of the story. ***The written feedback tells the rest.***

"It was nice to talk to someone that was knowledgeable and could understand."
– ITRC VICTIM

"She gave me critical information that I did not receive through any of the government websites I used or the identity protection company we hired. I'm so grateful for all of her help and support."
– ITRC VICTIM

[2] This reflects the self-determination by a victim that an issue reached a conclusion and is not based on any set criteria or definition.

Not all feedback reflects a resolved situation.

> *"I have severe anxiety, and the number of steps is overwhelming. I am also now facing financial hardship as a result of the fraud. I have felt unsupported until now."*
>
> **– ITRC VICTIM**

What stands out in this response is the final sentence. The victim had felt unsupported until they reached the ITRC. The crime was not resolved, but the experience of being heard and guided changed something.

The barriers respondents identified were rarely related to the quality of the ITRC's guidance, though the feedback is not without lessons for us. Four percent (4%) found the steps confusing, four percent (4%) found the number of steps overwhelming and three percent (3%) found the plan hard to follow. We are actively using this feedback to improve how we present recovery plans. Less than one percent (1%) said they didn't have time.

The more significant barriers to recovery are systemic and emotional: *institutions that don't respond, processes that take months and the exhaustion of fighting for something that was taken from you.*

Eighty-one percent (81%) of respondents across both surveys reported having taken the steps outlined in their recovery plans. This reflects two things:

- The clarity of the plans our advisors provide.
- The determination of the individuals who contact us.

Even when the system makes resolution difficult, people are willing to do the work. Our role is to make sure they know what that work looks like and that they don't have to figure it out alone.

> *"I feel better with the help and advice that the [ITRC Advisor] gave me. Feeling overwhelmed, I cannot think clearly, so this organization and the advisors were very compassionate and knowledgeable to help me. Without them, I would have been lost."*
>
> **– ITRC VICTIM**

Prevention & Response: **WHAT'S WORKING**

The Preemptive Consumer

How Victims Discover Identity Crime

Prevention & Response: WHAT'S WORKING

IDENTITY CRIME PREVENTION *is Often Framed as a Checklist*

☑ ***Freeze Your Credit*** ☑ ***Adopt Passkeys or Use Strong Passwords*** ☑ ***Enable Multi-Factor Authentication***

Those steps matter, and we recommend them. However, our data shows that prevention is more nuanced. Different crimes require different protections, and the most effective defenses depend on which type of crime a person is most likely to face.

This section examines what the data tells us about how people protect themselves, how they discover that something has gone wrong and which defenses catch identity crime before it causes lasting harm.

The PREEMPTIVE CONSUMER

Twelve percent (12%) of all cases reported to the ITRC this year (1,113 cases) came from individuals seeking information before a crime was confirmed, a 15.8 percent (15.8%) increase from the prior year. These individuals fall into three groups.

The largest group (68%) contacted us wanting additional information about identity protection or a potential concern. More than half of these individuals (51%) were unsure whether they were actually victims of misuse. They had received a suspicious notification, noticed something unusual or learned about a data breach affecting a company they used, and they wanted to know whether they needed to take action.

This is a meaningful shift: people are reaching out at the **FIRST SIGN THAT SOMETHING MIGHT BE WRONG.**

The second group (25%) had been targeted by a scam but did not share their personal information. These are individuals who recognized the scam in time and contacted the ITRC to report what happened and ask whether any additional steps were needed.

Their cases represent successful prevention efforts, and they provide valuable data on which scam types people are most likely to catch (as discussed in *Section I*).

The third group (7%) had lost physical items containing personal information, such as a wallet or phone, and contacted us to understand what protective steps to take before any misuse occurred.

Our quarterly data shows the share of preventative information requests growing over the reporting period, from 11.1 percent (11.1%) of cases in Q2 2025 to 12.4 percent (12.4%) in Q1 2026. The share of individuals wanting additional information also increased, from just under seven percent (6.7%) to nine percent (9%). These are trends worth watching. A growing, preemptive consumer base is a positive signal for prevention and reflects an increasing awareness that identity protection is not just something you address after the fact.

"I cannot thank you enough for your quick response and checklist of safeguards recommended. Without this information, I wouldn't have known what to do. You give me hope that the identity thieves stole. God bless."

– ITRC VICTIM

"We can't thank you enough. You made our job of preserving our identity, if not easy, doable, and with direction. Almost everything is back to normal. And if anything should come up in the future, we feel we are able to handle it. We would recommend the ITRC to all."

– ITRC VICTIM

How Victims **DISCOVER IDENTITY CRIME**

One of the most practical findings in this report is that the way a person discovers identity misuse is closely tied to the type of crime they are experiencing. This connection has direct implications for which protective measures are most effective against which threats.

Account Takeover

95%

Discovered Because Victim Was Unable to Log Into an Online Account

New Account Fraud

93%

Discovered By Victim Checking Their Credit Report

Criminal Identity Theft

77%

Victim Was Notified By Law Enforcement

Fraudulent Employment

83%

Discovered While Trying to Apply for Government Benefits

These are not coincidences. They reflect the structure of each crime type. Account takeover manifests as a lockout or unauthorized activity in an existing account. New financial account fraud manifests as an unfamiliar entry on a credit report. Criminal identity theft manifests through the criminal justice system. Fraudulent employment manifests through government benefits systems. Each crime has a different signal, and each signal requires a different monitoring behavior to detect it.

"Being older I was very happy [ITRC Advisor] was able to help me without me having to go to a bunch of Internet places I don't understand. I'm so thankful for people like [ITRC Advisor] for the understanding and patience for the older generation."

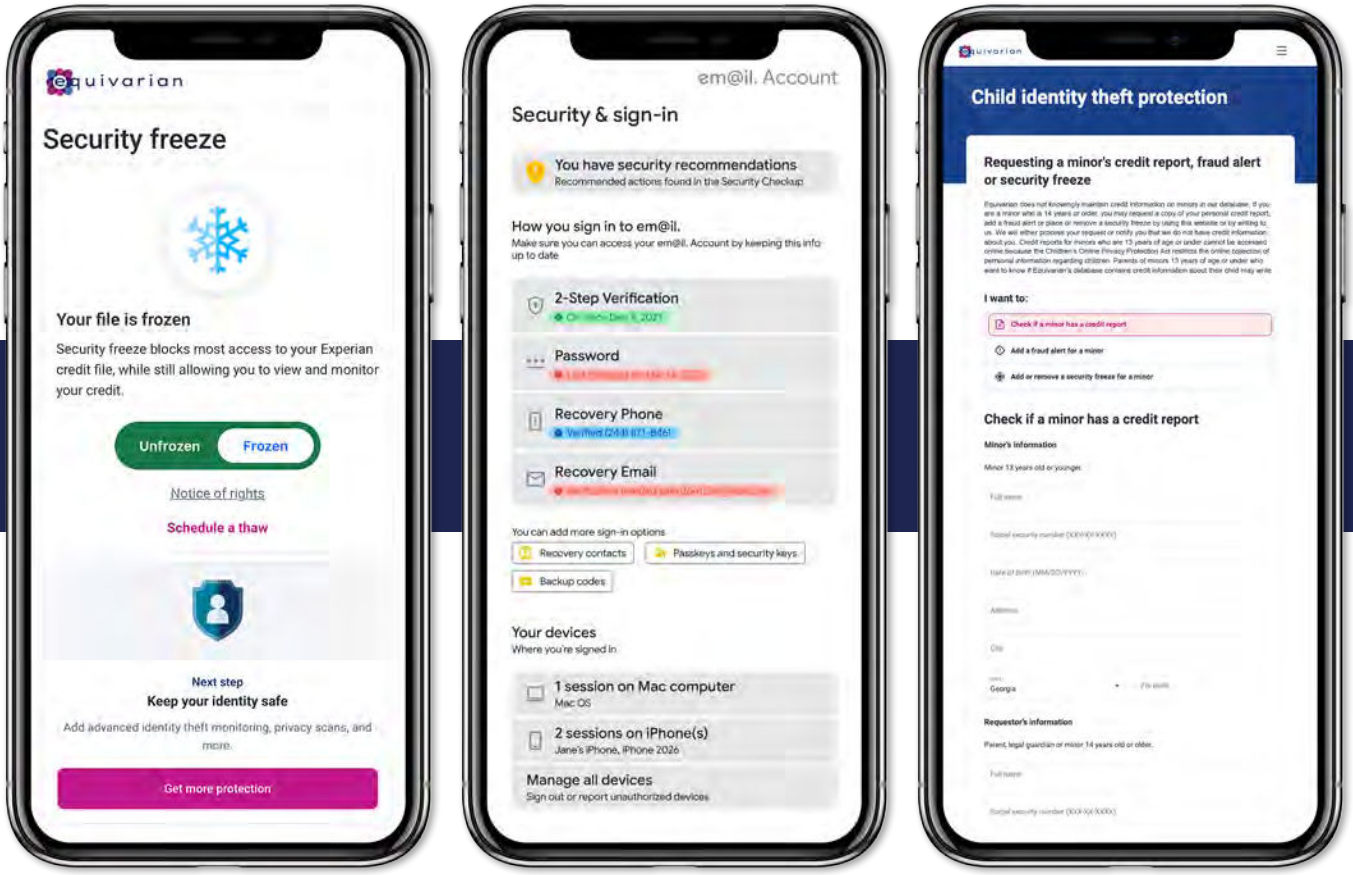
– ITRC VICTIM

The practical implication is that no single protective step catches everything. Checking your credit report is the most effective way to detect new financial account fraud (23 percent (23%) of all new account creation cases in our data were discovered this way), but it will not detect account takeover. Monitoring your account activity can catch account takeover, but it will not catch someone using your SSN for employment. Credit freezes prevent new accounts from being opened, but they do not protect existing accounts from being taken over.

Effective protection requires understanding: *which threats are most relevant to one's situation and which defenses should be layered to address them appropriately.*

For someone whose SSN was exposed in a data breach, a credit freeze and regular credit report monitoring address the most likely downstream risk (new financial account fraud).

For someone whose device was compromised, adopting passkeys or changing passwords, enabling multi-factor authentication (MFA) and reviewing active sessions across all accounts address the most likely risk (account takeover). For parents, freezing a child's credit, even if the child has no credit history yet, is the primary defense against fraudulent employment and new account fraud.



Geographical PATTERNS

Notable State Patterns

Geographical PATTERNS

The ITRC receives contacts from individuals across all 50 states, the District of Columbia and U.S. territories. While California, Texas and Florida generate the highest volume of cases (consistent with their population size), the more useful analysis is not where the most cases come from, but where the patterns differ from the overall data.

An important caveat: *state-level case counts in our data are influenced by referral partnerships, awareness of the ITRC and other factors beyond crime rates. The patterns described here reflect the experiences of individuals who contacted the ITRC from each state, not a comprehensive measure of identity crime prevalence in that state.*

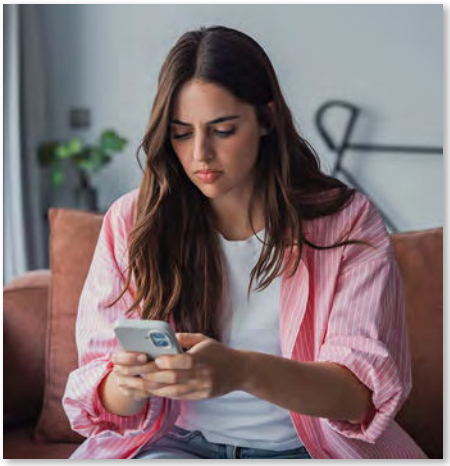
Full state-level data tables are available in the *Appendix*.

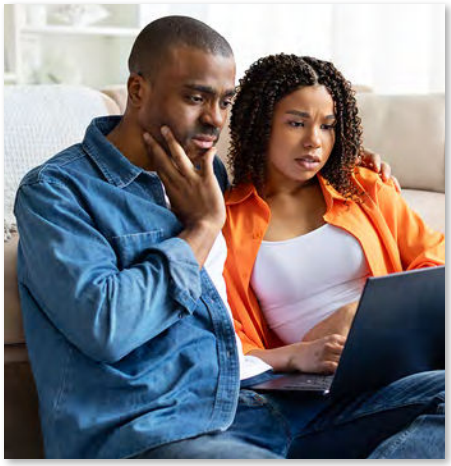
Notable STATE PATTERNS

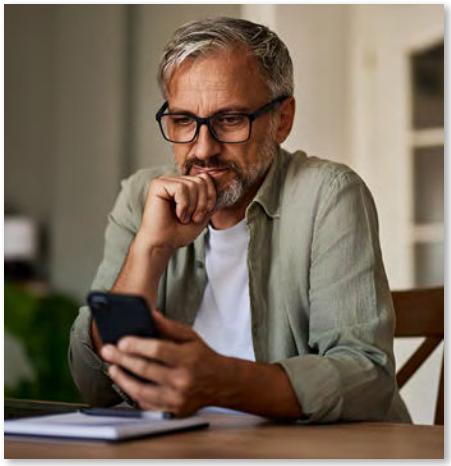
Several states showed identity crime profiles that deviated meaningfully from the overall data. We highlight the most distinctive here.

Colorado – *120 Cases, 61 Individuals*
Had the most distinctive profile in our data. Account takeover accounted for 40 percent (40%) of cases, 12 percentage points above the overall rate of 28 percent (28%). More strikingly, 49 percent (49%) of individuals from Colorado were managing multiple identity incidents, compared to 33 percent (33%) overall. Colorado also had an elevated attempted misuse rate (nine percent (9%) vs. four percent (4%) overall).

Tennessee – *126 Cases, 91 Individuals*
Stood out as the state with the most reported scams. Scam-related compromise accounted for 24 percent (24%) of cases, more than double the overall rate of 11 percent (11%). Among Tennessee's scam cases, "problems with the account" accounted for 42 percent (42%), followed by romance scams at ten percent (10%). Account takeover, conversely, was well below the overall rate at 19 percent (19%) compared to 28 percent (28%).







"I am very pleasantly surprised by the support and knowledge that [ITRC Advisor] passed on to me. I feel more secure in how to move forward. Very grateful."

– ITRC VICTIM

"I was very impressed with [ITRC Advisor], who made me feel heard and validated. I felt like she completely understood what I was going through. That, in and of itself, was priceless to me, as my friends and family were sympathetic but really couldn't empathize. The information she provided was so valuable, and I took action to do all the steps that were recommended."

– ITRC VICTIM

"You answered all my questions and offered me the option of reaching out to you again should any questions or issues arise. I felt like you guys really cared."

– ITRC VICTIM

"The advisor was so helpful, and she understands what I am going through. She is extremely helpful and very understanding, and provided me with helpful resources."

– ITRC VICTIM

Illinois – *180 Cases, 109 Individuals*
Had the highest rate of fraudulent employment at nine percent (9%), nearly three times the overall rate of three percent (3%). New account fraud was also elevated at 32 percent (32%) (vs. 26 percent (26%) overall), while compromise cases were notably lower at 20 percent (20%) (vs. 29 percent (29%) overall).

Virginia – *127 Cases, 73 Individuals*
Reported the highest data breach rate at nine percent (9%), three times the overall rate of three percent (3%). Virginia is home to a significant concentration of federal government and defense contractors, which may contribute to a population more likely to be affected by institutional data breaches. Job and employment scams led Virginia's scam cases at 30 percent (30%), also well above typical levels.

Michigan – *125 Cases, 84 Individuals*
Had the highest device access rate at 14 percent (14%) of cases, nearly double the overall rate of eight percent (8%). Michigan also had a higher share of compromise cases overall (37 percent (37%) vs. 29 percent (29%)) and a lower share of misuse cases (46 percent (46%) vs. 58 percent (58%)).

Florida – *413 Cases, 247 Individuals*
Showed an elevated account takeover rate at 35 percent (35%) (vs. 28 percent (28%) overall), while new account fraud was below average at 21 percent (21%) (vs. 26 percent (26%)). Among Florida's scam cases, tech support scams accounted for 16 percent (16%), well above their overall share.

METHODOLOGY

Data Source & Scope

All data in this report is based on individuals who contacted the ITRC between April 1, 2025, and March 31, 2026. During this period, the ITRC received 9,253 cases from 6,188 unique individuals. Contacts were received by phone, chat, email, text-to-chat, web form and letter.

This data reflects the experiences of individuals who chose to contact the ITRC. It is not a random sample of all identity crime victims and should not be interpreted as a measure of identity crime prevalence in the United States. The individuals in our data found the ITRC through referral partners, online searches, government agencies, financial institutions and other channels. Their experiences may differ from those of individuals who did not contact the ITRC or who sought assistance elsewhere.

Case & Contact Structure

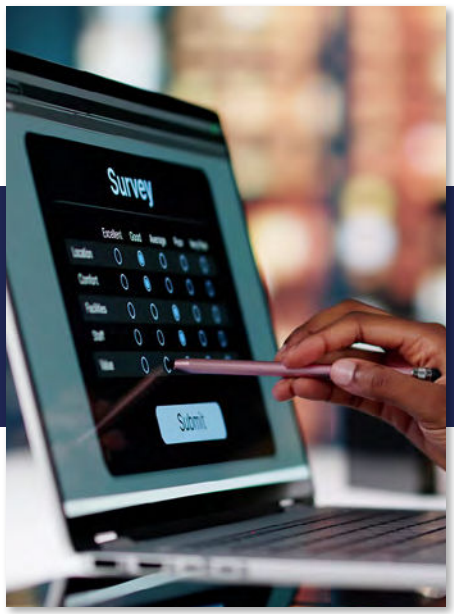
Each individual who contacts the ITRC is assigned a unique contact record. A single individual may have multiple cases if they are experiencing more than one identity-related incident. The 9,253 cases from 6,188 individuals reflect this structure: 74.4 percent (74.4%) of individuals had a single case, while 25.6 percent (25.6%) had two or more.

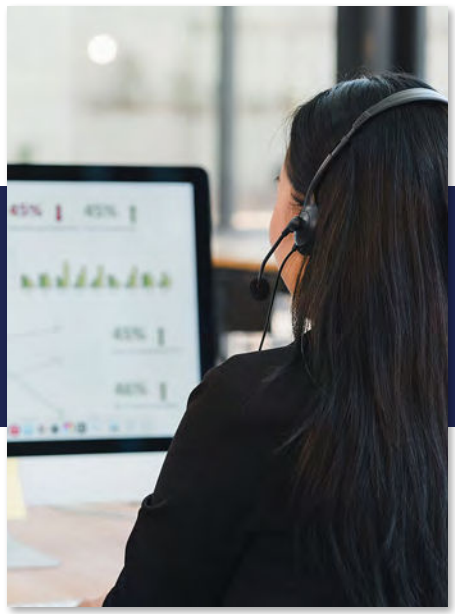
The ITRC categorizes cases into four primary categories based on the individual's reason for contacting us: misuse (54.3%), compromise (30.3%), attempted misuse (3.4%) and requests for preventative information (12%).

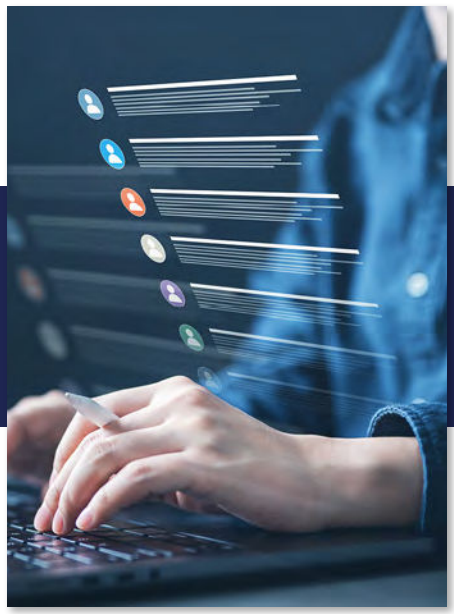
Demographic Data

Demographic information, including age, gender, household income and ethnicity, is collected on a voluntary basis. Response rates vary by field: age (43 percent (43%) of individuals), gender (38%), ethnicity (37%) and household income (30%). These rates exclude individuals who selected "Decline to State." Targeted population data (such as domestic violence survivor, formerly incarcerated or experiencing homelessness) is self-identified.

Since demographic data is voluntary, the individuals who provided this information may not be representative of all individuals who contacted the ITRC. Demographic findings in this report should be understood as describing patterns among those who chose to share this information.







Survey Data

Three surveys were administered during the reporting period:

- ***The Emotional Impact Survey*** (261 respondents) collected information on the emotional effects of identity crime, including specific emotions experienced, whether the individual sought emotional support and whether their concern was resolved.
- ***The Financial Impact Survey*** (147 respondents) collected information on the financial consequences of identity crime, including specific financial hardships, coping mechanisms and resolution status.
- ***The Victim Services Satisfaction Survey*** (236 respondents) collected information on the individual's experience working with an ITRC advisor, including satisfaction ratings, perceived advisor knowledge and dedication, comfort with the recovery plan and barriers to taking recommended steps.

All three surveys were voluntary and self-selected. Respondents may not represent all individuals who contacted the ITRC. Survey findings are presented as descriptive patterns rather than population-level statistics.

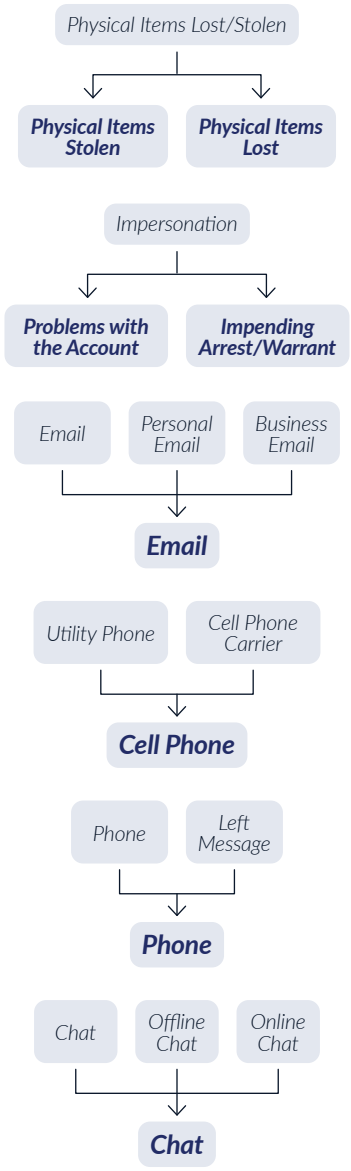
Compromise-to-Misuse Pipeline Analysis

Section II of this report examines the 395 individuals who experienced both a compromise and subsequent misuse during the reporting period. This analysis uses data from the "Contacts with Comp+Misuse" dataset, which links compromise and misuse cases for the same individual, allowing us to trace the pathway from exposure to use.

Data Entry & Classification

Case data is entered by ITRC Identity Theft Advisors during or immediately following victim interactions. Several classification changes were implemented during this reporting period that affect year-over-year comparisons.

- *"Physical Items Lost/Stolen"* was separated into two categories: ***"Physical Items Stolen"*** (classified as compromise) and ***"Physical Items Lost"*** (classified as preventative information). Prior-year data used a combined category.
- Scam type classification was refined to capture specific scam pretexts (such as ***"problems with the account"*** or ***"impending arrest/warrant"***) rather than the broader *"impersonation"* category used in prior years. This change provides more detailed data on how scams operate but limits direct year-over-year comparisons for individual scam types.
- Email account types (email, email-personal, email-business) were combined into a single ***"email"*** category. Utility-phone and cell phone carrier were combined into ***"cell phone carrier."*** For contact methods, phone and left message were combined into ***"phone,"*** and chat, offline chat and online chat were combined into ***"chat."***



Year-Over-Year Comparisons

Where year-over-year comparisons appear in this report, the prior-year data refers to the period April 1, 2024, through March 31, 2025 (9,031 cases from 6,405 individuals). Year-over-year percentage changes are calculated from the prior-year baseline.

Quarterly Trend Analysis

Intra-period quarterly trends referenced in this report are estimated using linear interpolation of case numbers to opened dates, based on a subset of cases with known dates (r = 0.9985 correlation). Quarter boundaries are Q2 2025 (April through June), Q3 2025 (July through September), Q4 2025 (October through December) and Q1 2026 (January through March). Quarterly trends reflect shifts in percentage share within the reporting period and should be interpreted as directional patterns rather than precise measurements.

GLOSSARY

Since 2020, the ITRC has published the definitions we use in compiling and publishing this report.

Attack Vector	The category of method used by a threat actor to compromise an organization's data. + ***Cyberattacks*** *involve compromising an electronic information system using software or computer technology.* + ***Physical attacks*** *involve compromising data through a physical act.* + ***System or Human Errors*** *are failures of a system or human being to perform as expected or required without malicious intent that results in a data compromise.*
Data Breach	When unauthorized individuals access and/or remove personal information from the place where it is stored.
Data Compromise/Event	The overall term used to refer to events where personal information is accessible by unauthorized individuals and/or for unintended purposes. This includes data breaches, data exposures and data leaks.
Data Exposure	When personal information is available for access and/or removal from the place where it is stored, but there is no evidence the information has been accessed by unauthorized individuals. This typically involves cloud-based data storage where cybersecurity protections are incorrectly configured or have not been applied.
Data Leak	When personal information that is publicly available or willingly shared on social media and represents no or low risk when viewed as individual records; however, when aggregated, the sheer volume of personal information available in a single database creates risk to the data subjects and value for identity criminals who specialize in social engineering and phishing. When these databases are left unprotected or otherwise made publicly available, the ITRC classifies these events as Data Leaks.
Identity Crimes	The overall term for a wide variety of state and federal criminal acts that are related to the theft and/or misuse of personal information.

Identity Fraud	Using stolen personally identifiable information (PII).
Identity Theft	Taking personally identifiable information (PII) as protected by state or federal laws.
Industry	Standard categories used to filter data compromises by organization type/sector and industry (based on SIC code).
Non-Sensitive Records	Non-sensitive personal information (PII) as defined by statute, such as telephone numbers, email addresses, login and passwords, etc.
Previously Compromised Data (PCD)	Refers to information that was stolen in past data breaches and later repackaged, aggregated or recirculated – often without new breach notifications.
Sensitive Records	Sensitive personal identifiable information (SPII) as defined by statute, such as passport numbers, SSN, driver's license, health information, etc.
Threat Actor	A threat actor is the person or group whose malicious actions results in a data compromise. Internal actors are employees of a compromised organization. An external actor may be an independent person or group. A Nation/State actor is acting on behalf of a government.
Unknown Records	Type of records compromised are unknown.
Victim Notices	The ITRC reports the number of Victim Notices for both individual events and as a total for all reported compromises as a measure of the scale of events and impacts on individuals. However, Victim Notices should not be considered a 1-to-1 count of actual victims since not all notices include a victim count, and those that do may not reflect the number of individuals impacted, but rather the number of accounts compromised including instances where a person has multiple accounts. Aggregated totals also inflate the number of individuals affected because of single individuals receiving breach notices from multiple events.

ADVISORY *Board*

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
Matrix Ventures

JAY MEIER
VICE CHAIR
Chief Identity Technology Strategist, FaceTec, Inc.

KRIS BOSSOWSKI
ADVISOR
Federal Agent, U.S. Government Law Enforcement Agency

KERRY CANTLEY
ADVISOR
Vice President of Digital Banking Strategy, Mitek

PAYAM HOJJAT
ADVISOR
Cybersecurity Risk & Governance Chief, State of CA

MEGHAN LAND
ADVISOR
Executive Director, Privacy Rights Clearinghouse

ADAM LEVIN
ADVISOR
Consumer Affairs Advocate & Serial Entrepreneur

AARON MENDES
ADVISOR
CEO & Co-Founder, PrivacyHawk

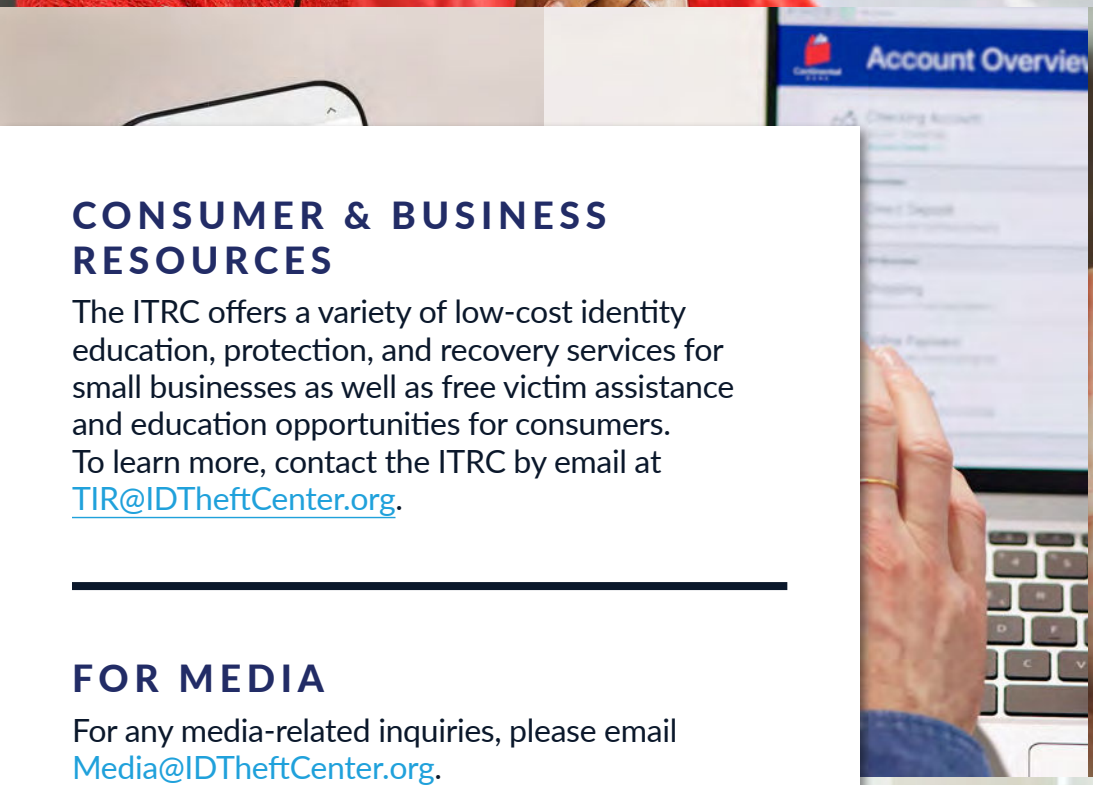
LYNETTE OWENS
ADVISOR
VP of Global Consumer Education & Product Marketing, Trend Micro

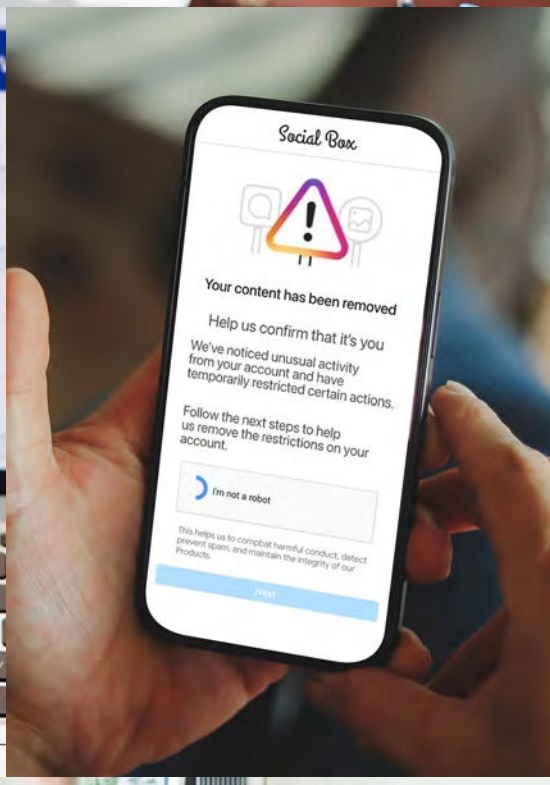
LISA PLAGGEMIER
ADVISOR
Executive Director, National Cybersecurity Alliance

TIR

IDENTITY THEFT RESOURCE CENTER

2026 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, contact the ITRC by email at TIR@IDTheftCenter.org.

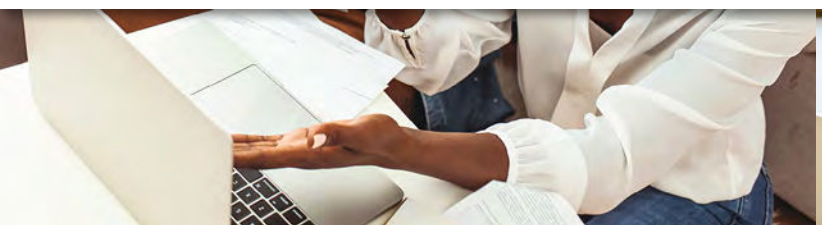
FOR MEDIA

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

CONTRIBUTORS

Thanks to the team responsible for the *2026 ITRC Trends in Identity Report*:

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



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 2026

APPENDIX

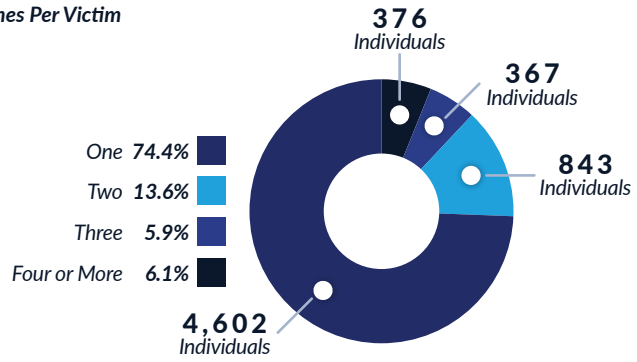
APPENDIX

EXECUTIVE SUMMARY

Key Metrics

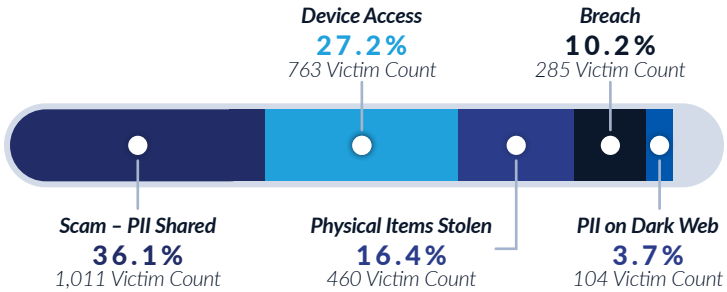
	2025-2026	2024-2025	Year-Over-Year Change
Total Cases	**9,253**	**9,031**	**2.5%**
Unique Contacts	6,188	6,405	-3.4%
Misuse Cases	5,020	4,681	7.2%
Compromise Cases	2,803	3,139	-10.7%
Attempted Misuse	317	250	26.8%
Preventative Info	1,113	961	15.8%

Crimes Per Victim



COMPROMISE

Compromise By Type



Stolen Items Reported

	Count	Percentage
Driver's License/State I.D.	61	11.4%
Phone/Tablet	41	7.7%
Credit/Payment Card(s)	36	6.8%
Social Security Card	33	6.2%
Driver's License/State I.D.; Social Security Card	32	6.0%
Birth Certificate; Social Security Card	27	5.1%
Documents-Other	27	5.1%
Mail	21	3.9%
Birth Certificate; Driver's License/State I.D.; Social Security Card	17	3.2%
Payment/Refund Check	15	2.8%

Scam Types

	Count	Percentage
Problems With the Account	340	26.4%
Job/Employment	147	11.4%
Unknown	98	7.6%
Lottery/Prize	97	7.5%
Impending Arrest/Warrant	87	6.8%
Sale of Goods/Services	79	6.1%
Tech Support	66	5.1%
Romance	63	4.9%
Impersonation	63	4.9%
New/Past Due Invoice	55	4.3%
Cryptocurrency	30	2.3%
Other	29	2.3%
Total	**1,286**	

Who Scammers Pretend to Be

	Count	Percentage
Business	562	49.1%
Financial Institution	162	14.2%
Potential Employer/Job Recruiter	104	9.1%
Federal/State Agency	67	5.9%
Federal Agency	63	5.5%
Potential Partner/Partner	41	3.6%
Celebrity	36	3.1%
Charity	19	1.7%
Potential Landlord	18	1.6%
Police/Sheriff	17	1.5%

Companies/Agencies Impersonated

	Count
PayPal	39
American Express (AMEX)	35
Amazon	31
Publishers Clearing House- PCH	28
Dish Network	27
Microsoft	25
Department of Homeland Security (DHS)	21
Social Security Administration (SSA)	20
Apple Support	17
Bank of America	17

Attempted Misuse By Account Type

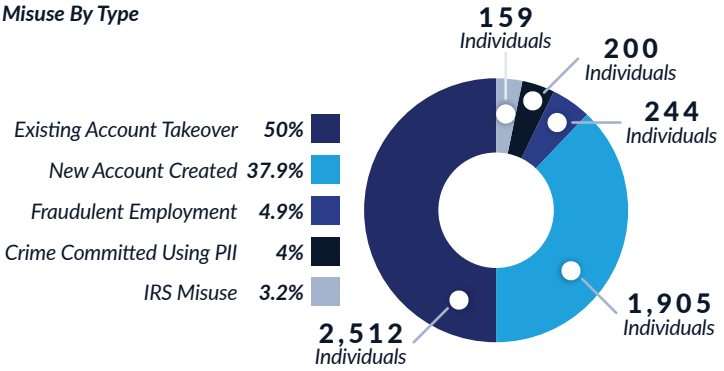
	Count	Percentage
Credit Card	130	41.0%
Bank-Checking	56	17.7%
Personal Loan	27	8.5%
Auto Loan	16	5.0%
P2P Payment App	13	4.1%
Cell Phone Carrier	11	3.5%
Mortgage Loan	10	3.2%
Social Media	6	1.9%
Email	5	1.6%
Merchant	4	1.3%

Scam Recognition Rate

	Total	Not Shared	Recognition Rate
New/Past Due Invoice	55	35	63.6%
Impersonation	63	27	42.9%
Lottery/Prize	97	41	42.3%
Impending Arrest/Warrant	87	26	29.9%
Other	29	8	27.6%
Cryptocurrency	30	5	16.7%
Problems With the Account	340	52	15.3%
Sale of Goods/Services	79	12	15.2%
Romance	63	9	14.3%
Unknown	98	11	11.2%
Tech Support	66	6	9.1%
Job/Employment	147	12	8.2%

MISUSE

Misuse By Type

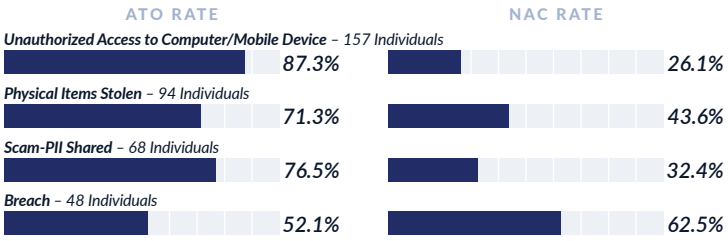


ATO By Account Type

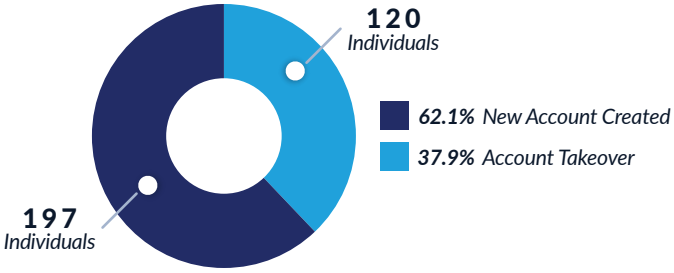
	Count	Percentage
Bank-Checking	635	25.3%
Credit Card	470	18.7%
Email	338	13.5%
Social Media	229	9.1%
Cell Phone Carrier	132	5.3%
P2P Payment App	79	3.1%
Personal Tech Account	69	2.7%
Merchant	67	2.7%
CRA	67	2.7%
Insurance-Medical	42	1.7%
DMV	41	1.6%
Bank-Savings	38	1.5%
IRS	35	1.4%
Investment	29	1.2%
Other	20	0.8%

PIPELINE

Compromise – Misuse Conversion



Attempted Misuse



NAC By Account Type

	Count	Percentage
Credit Card	623	32.7%
Bank-Checking	181	9.5%
Personal Loan	153	8.0%
Cell Phone Carrier	102	5.4%
Auto Loan	97	5.1%
Mortgage Loan	86	4.5%
Student Loan-Federal	53	2.8%
Property Lease/Rental	45	2.4%
Unemployment	45	2.4%
Medical Provider	43	2.3%
Other	36	1.9%
DMV	34	1.8%
Insurance-Medical	33	1.7%
Utility-Electricity	33	1.7%
P2P Payment App	29	1.5%

Discovery Method By Misuse Type

EXISTING ACCOUNT TAKEOVER

	Count	Percentage
Checked Own Account	690	28.4%
Unknown	653	26.9%
Notified By Account Issuer/Holder	541	22.3%
Unable to Login to Online Account(s)	480	19.8%

NEW ACCOUNT CREATED

	Count	Percentage
Notified By Account Issuer/Holder	610	33.1%
Unknown	509	27.6%
Checked Credit Report	422	22.9%
Received Notice	78	4.2%

FRAUDULENT EMPLOYMENT

	Count	Percentage
Applying for State/Federal Benefits	54	22.6%
Government Agency	45	18.8%
Unknown	36	15.1%
Notified By Account Issuer/Holder	32	13.4%

IRS MISUSE

	Count	Percentage
Notified By Account Issuer/Holder	56	36.1%
Unknown	46	29.7%
Government Agency	38	24.5%
Checked Own Account	11	7.1%

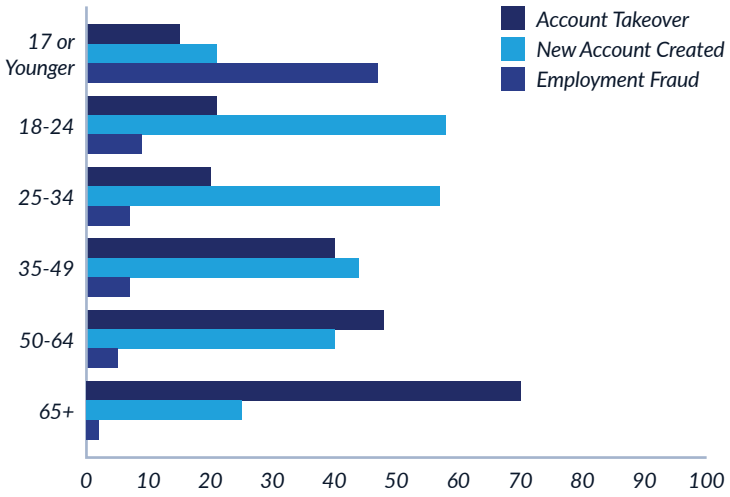
CRIME COMMITTED USING PII

	Count	Percentage
Notified By Law Enforcement	61	33.5%
Unknown	50	27.5%
Obtained a Background Check	26	14.3%
Notified By Account Issuer/Holder	19	10.4%

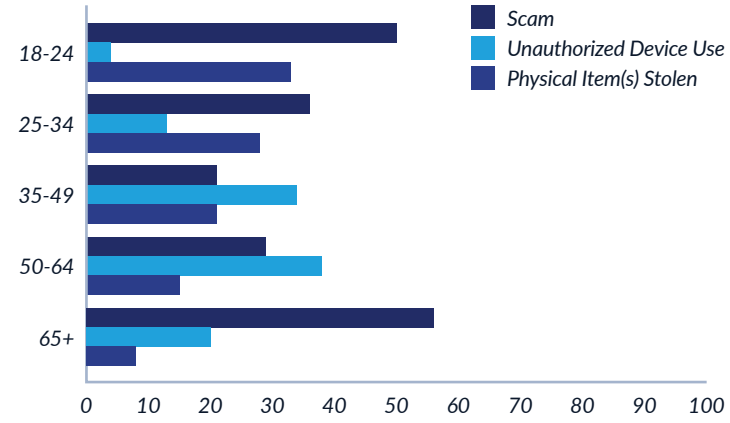
IRS Misuse Detail

	Count	Percentage
Taxes Filed Using Victim's Information	135	85.4%
Fraudulently Claimed as Dependent	15	9.5%
Contact/Bank Information Changed	4	2.5%
Refund Not Received	2	1.3%
Tax Credit/Stimulus Payment Not Received	2	1.3%

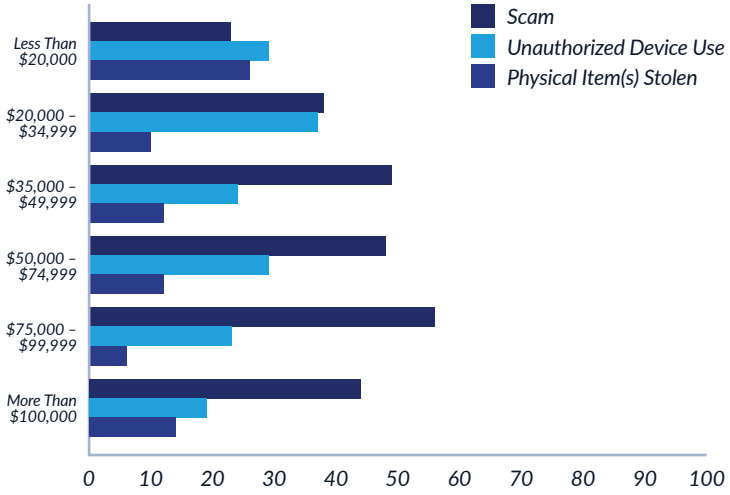
Age + Misuse Type



Age + Compromise Type



Income + Compromise Type



Income + Misuse Type

Alleged Thief

	Percentage
Unknown	85.8%
Ex-Spouse/Partner	4.8%
Friend	1.7%
Family-Extended	1.7%
Other	1.6%
Spouse/Partner	1.2%
Neighbor	0.8%
Family-Parent	0.7%
Trafficker	0.6%
Family-Sibling	0.6%
Child/Dependent	0.3%
Family-Grandparent	0.1%

Targeted Populations

	Cases
Domestic Violence Survivor	270
Incarcerated - Former	109
Homeless	101
Trafficking Survivor	92
Blind/Vision Impaired	47
Deaf/Hearing Impaired	40
Former/Foster Youth	35
Military - Veteran	32
Veteran	15
Military - Active Duty	9
Incarcerated - Current	3

Victim

	Percentage
Self	91.9%
Child/Dependent	2.0%
Spouse/Partner	2.0%
Family-Parent	1.1%
Child/Dependent- Adult	0.7%
Friend	0.3%
Family-Sibling	0.3%
Deceased	0.3%
Business/Non-Profit	0.2%
Client-Advocate	0.2%
Family-Extended	0.2%
Deceased; Family-Parent	0.2%

HUMAN IMPACT

Emotional Impact – Prevalence

	Count	Percentage
Frustrated	189	73.5%
Anxious	181	70.4%
Worried	180	70.0%
Angry	179	69.6%
Violated	156	60.7%
Vulnerable	137	53.3%
Like I Can't Trust People	136	52.9%
Depressed	118	45.9%
Sad	116	45.1%
Unsafe	112	43.6%
Guilt/Shame That I Made This Happen, or I Did Something Wrong	104	40.5%
Suicidal	25	9.7%

Emotional Impact By Crime Type

	Count	Average Emotions	Guilt Percentage	Depression Percentage	Suicidal Percentage
Existing Account Takeover	52	7.0	32.7%	55.8%	7.7%
Scam-PII Shared	65	5.5	56.9%	33.8%	6.2%
New Account Created	44	6.3	29.5%	43.2%	11.4%
Crime Was Committed Using PII	7	8.0	28.6%	57.1%	42.9%
Fraudulent Employment	9	8.1	44.4%	88.9%	11.1%

Financial Impact – Consequences

	Count	Percentage
None of the Above	63	45.3%
Now in Debt	49	35.3%
Unable to Pay Regular Bills	43	30.9%
Denied Credit or Loans	40	28.8%
Other	34	24.5%
Used Savings to Pay for Expenses	29	20.9%
Unable to Pay Rent	29	20.9%
Denied a Checking Account	21	15.1%
Forced to Declare Bankruptcy	6	4.3%

Financial Impact – Coping

	Count	Percentage
It Was Not Difficult for Me to Meet My Financial Needs	49	36.8%
Went Without	48	36.1%
Other	41	30.8%
Borrowed Money From Friends and/or Family	27	20.3%
Used One or More Credit Cards	22	16.5%
Sought Government Assistance	19	14.3%
Obtained a Payday Loan	5	3.8%
Obtained a Loan From a Bank, Credit Union or Other Financial Institution	5	3.8%

Satisfactory Survey – Rated 4 or 5 Out of 5, 236 Total Respondents

Satisfied With Advisor – 212 Individuals
89.8%

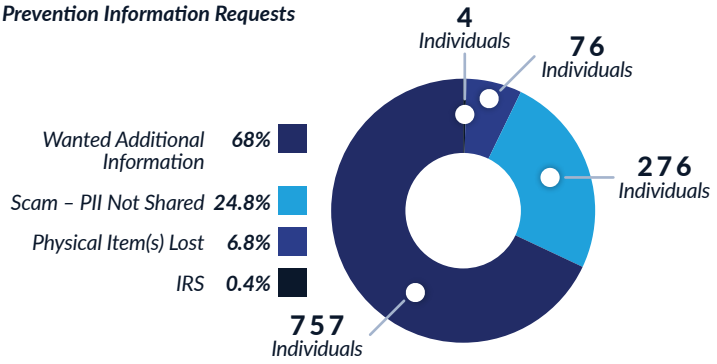
Advisor Dedication – 208 Individuals
88.1%

Knowledgeable Advisor – 209 Individuals
88.6%

Comfortable Case Plan – 197 Individuals
83.5%

PREVENTION

Prevention Information Requests

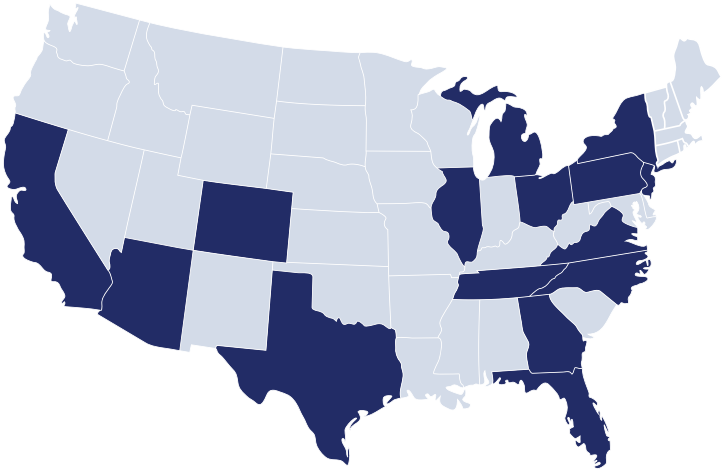


Discovery Method – Crime Type

	Cases	Top Crime	Match Percentage
Unable to Login to Online Account(s)	507	Existing Account Takeover	94.7%
Checked Credit Report	452	New Account Created	93.4%
Notified By Law Enforcement	79	Crime Committed Using PII	77.2%
Applying for State/Federal Benefits	65	Fraudulent Employment	83.1%
Checked Own Account	791	Existing Account Takeover	87.2%
Notified By Account Issuer/Holder	1,258	New Account Created	48.5%
Sent Collections Notice	84	New Account Created	83.3%
Credit/ID Theft Monitoring	39	New Account Created	92.3%

GEOGRAPHIC

Prevention Information Requests



	Cases	Individuals	Misuse Percentage	Compromise Percentage	ATO Percentage	NAC Percentage	Scam Percentage
California	1,117	675	59.5%	29.3%	30.0%	25.6%	10.7%
Texas	460	285	64.1%	23.0%	25.4%	30.2%	8.9%
Florida	413	247	58.8%	28.1%	35.1%	20.6%	12.1%
New York	322	201	55.0%	32.9%	29.8%	22.4%	13.7%
Georgia	188	93	62.2%	21.8%	34.6%	23.9%	6.9%
North Carolina	185	110	54.6%	31.9%	30.8%	24.9%	14.1%
Arizona	180	93	57.8%	30.0%	31.1%	20.0%	10.6%
Illinois	180	109	65.6%	20.0%	26.1%	31.7%	8.3%
Pennsylvania	156	100	53.2%	30.8%	29.5%	28.2%	10.3%
Ohio	153	88	50.3%	34.6%	20.9%	30.1%	12.4%
New Jersey	133	71	57.9%	28.6%	30.1%	28.6%	11.3%
Virginia	127	73	52.8%	33.9%	24.4%	27.6%	13.4%
Tennessee	126	91	51.6%	34.9%	19.0%	27.8%	23.8%
Michigan	125	84	46.4%	36.8%	25.6%	23.2%	9.6%
Colorado	120	61	57.5%	27.5%	40.0%	22.5%	9.2%

GENDER

Gender + Misuse Type

	Cases	ATO Percentage	NAC Percentage	Crime Using PII Percentage
Female	1,399	47.4%	37.6%	3.1%
Male	982	41.6%	43.9%	6.6%

ETHNICITY

Ethnicity + Misuse Type

	Cases	ATO Percentage	NAC Percentage	Employment Fraud Percentage	Crime Using PII Percentage
White	1,140	52.8%	36.9%	3.8%	2.8%
Black or African American	397	37.3%	45.1%	5.0%	7.6%
Hispanic, Latino, Spanish Origin	389	27.5%	45.8%	14.7%	9.3%
Asian	92	43.5%	45.7%	8.7%	1.1%
Two or More Races	138	38.4%	48.6%	5.8%	2.2%
American Indian, Alaskan Native	46	28.3%	54.3%	10.9%	0.0%

Ethnicity + Compromise Type

	Cases	Scam Percentage	Unauthorized Device Use Percentage	Physical Item Stolen Percentage	Breach Percentage
White	658	40.7%	29.8%	12.2%	7.9%
Black or African American	165	29.1%	27.3%	27.3%	6.7%
Hispanic, Latino, Spanish Origin	135	34.1%	25.2%	23.7%	6.7%
Asian	61	60.7%	13.1%	8.2%	8.2%
Two or More Races	55	27.3%	27.3%	23.6%	14.5%
American Indian, Alaskan Native	22	22.7%	22.7%	22.7%	27.3%

ALL STATES

All States, Crime Category

	Cases	Individuals	Misuse Percentage	Compromise Percentage	Attempted Misuse Percentage	Prevention Percentage
CA	1,117	675	59.5%	29.3%	3.8%	7.3%
TX	460	285	64.1%	23.0%	3.5%	9.3%
FL	413	247	58.8%	28.1%	3.9%	9.2%
NY	322	201	55.0%	32.9%	2.5%	9.6%
GA	188	93	62.2%	21.8%	6.4%	9.6%
NC	185	110	54.6%	31.9%	4.9%	8.6%
AZ	180	93	57.8%	30.0%	3.3%	8.9%
IL	180	109	65.6%	20.0%	6.1%	8.3%
PA	156	100	53.2%	30.8%	9.0%	7.1%
OH	153	88	50.3%	34.6%	6.5%	8.5%
NJ	133	71	57.9%	28.6%	6.0%	7.5%
VA	127	73	52.8%	33.9%	6.3%	7.1%
TN	126	91	51.6%	34.9%	2.4%	11.1%
MI	125	84	46.4%	36.8%	4.8%	12.0%
CO	120	61	57.5%	27.5%	9.2%	5.8%
MD	111	69	53.2%	35.1%	3.6%	8.1%
IN	107	64	57.9%	28.0%	3.7%	10.3%
WA	107	70	57.9%	29.9%	1.9%	10.3%
SC	99	59	49.5%	36.4%	3.0%	11.1%
MA	94	58	55.3%	31.9%	2.1%	10.6%
OR	89	55	61.8%	27.0%	2.2%	9.0%
LA	87	51	64.4%	24.1%	2.3%	9.2%
MO	85	56	48.2%	32.9%	3.5%	15.3%
MN	76	52	56.6%	26.3%	2.6%	14.5%
NM	75	54	53.3%	33.3%	1.3%	12.0%
NV	72	39	59.7%	30.6%	0.0%	9.7%
WI	71	46	54.9%	35.2%	2.8%	7.0%
OK	70	36	61.4%	28.6%	4.3%	5.7%
KY	64	38	40.6%	35.9%	6.3%	17.2%
AR	59	40	45.8%	44.1%	0.0%	10.2%
KS	56	28	66.1%	25.0%	1.8%	7.1%
AL	52	32	61.5%	25.0%	3.8%	9.6%
ID	51	29	58.8%	19.6%	7.8%	13.7%
UT	48	30	60.4%	29.2%	0.0%	10.4%
OTH	48	41	60.4%	20.8%	4.2%	14.6%
DC	46	22	80.4%	10.9%	2.2%	6.5%
CT	39	29	56.4%	23.1%	2.6%	17.9%
MS	34	25	47.1%	44.1%	2.9%	5.9%
NE	31	13	54.8%	29.0%	12.9%	3.2%
IA	28	18	60.7%	35.7%	0.0%	3.6%
DE	27	15	77.8%	22.2%	0.0%	0.0%
INV	27	21	59.3%	22.2%	3.7%	14.8%
WV	24	12	66.7%	25.0%	4.2%	4.2%
ME	18	13	55.6%	27.8%	0.0%	16.7%
NH	15	9	66.7%	26.7%	6.7%	0.0%
ND	13	8	69.2%	30.8%	0.0%	0.0%
RI	12	8	66.7%	16.7%	0.0%	16.7%
HI	11	7	36.4%	54.5%	0.0%	9.1%
MT	9	8	11.1%	44.4%	0.0%	44.4%
SD	7	4	100.0%	0.0%	0.0%	0.0%
AK	6	5	33.3%	66.7%	0.0%	0.0%
VT	5	3	60.0%	40.0%	0.0%	0.0%
WY	4	3	50.0%	25.0%	0.0%	25.0%
Ca	1	1	0.0%	0.0%	0.0%	100.0%

CONTACTS & REFERRALS

Contact Method (Combined)

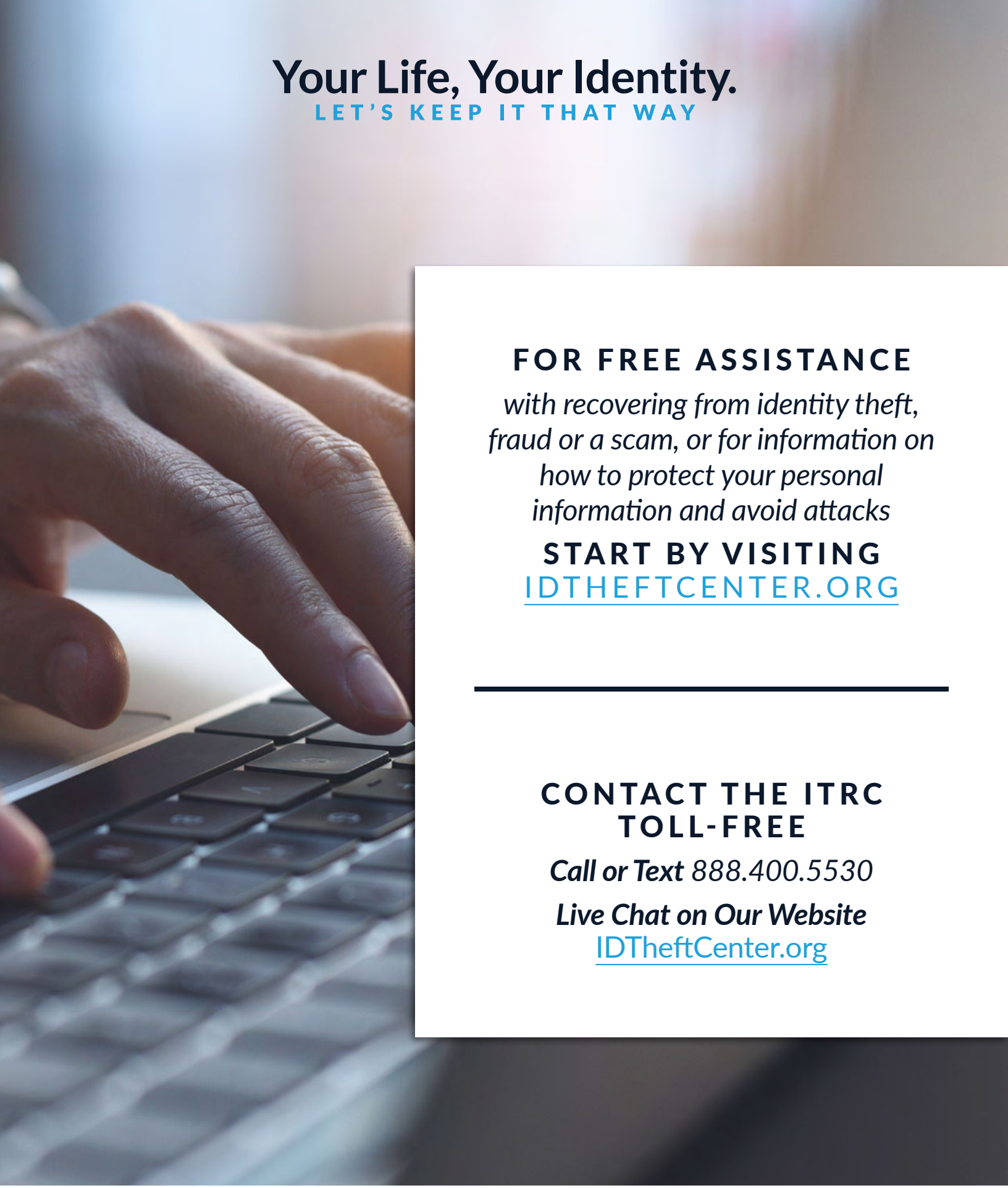
	Cases	Percentage
Phone	6,978	75.4%
Chat	1,745	18.9%
Email	259	2.8%
Text-To-Chat	184	2.0%
Web Form	77	0.8%
Letter	7	0.1%

Referred to ITRC By

	Cases	*Percentage*
Search Engine	2,500	33.5%
Unknown	1,567	21.0%
Federal Government Agency	755	10.1%
ITRC Website	519	7.0%
Tier 2	448	6.0%
NGO/Advocate	390	5.2%
Financial Institution	303	4.1%
Local Law Enforcement	239	3.2%
Business	167	2.2%
State Government Agency	124	1.7%
Friend/Family Member	118	1.6%
Media Story	93	1.2%
Social Media Company	65	0.9%
Prior Victim	51	0.7%
211	44	0.6%
CRA	40	0.5%
ITRC Social Media/Podcast	20	0.3%
County Government Agency	18	0.2%
ITRC Webinar/Presentation	4	0.1%

Top Referral Organizations

	Cases
Google	1,317
Federal Trade Commission (FTC)-Identity Theft	548
American Express (AMEX)	396
National Consumers League (NCL) Fraud.org	123
Synchrony Bank	112
Bank of America	97
New Mexico Department of Justice	67
National Cybersecurity Alliance (Stay Safe Online) (srcdoc)	53
Duck Duck Go	42
Dish Network	39
Social Security Administration (SSA)	38
San Jose Police Department (SJPD)	38
ChatGPT (OpenAI)	36
Federal Bureau of Investigations (IC3)	35
Bing (Microsoft)	31



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