# Identity Theft Resource Center 2024 Predictions

## A Recap of the ITRC's 2023 Predictions

+ **Prediction #1** - Identity criminals will increasingly rely on impersonation using personally identifying information (PII) gathered through compromises, phishing and social engineering to open new accounts, take over non-financial accounts such as social media, and impersonate government representatives.
    - » ***Result*** - Bingo! Cybercriminals gained control over existing accounts or opened new accounts 93 percent of the time when victims contacted the ITRC about credentials being misused. Opening new state government benefits and new financial accounts were the most commonly reported compromise.
+ **Prediction #2** - Romance scams will continue to morph into relationship scams.
    - » ***Result*** - Spot on! The ITRC continued to hear heart-breaking examples of people being defrauded as part of a long-con scam where the criminal built a relationship over time before asking for funds – oftentimes in the form of cryptocurrency. These relationships did not always have a romantic component. Connection of all sorts was the key. We also noted a significant rise in the number of victims who lost six figures. These scams also tended to involve cryptocurrency and cryptocurrency ATMs.
+ **Prediction #3** - Scams targeting specific racial and ethnic groups or immigrants who have limited English proficiency will increase.
    - » ***Result*** - Yes, but more study is needed. After a two-year research project by the ITRC and partners, we now know that Black communities are victimized at a higher rate and the impacts are greater than the general U.S. population. We're seeking partners to conduct similar studies in other distinct communities.
+ **Prediction #4** - Identity criminals will move to exploit the technology gap between people who adopt passkeys and other passwordless tech and those who can't or won't make the shift.
    - » ***Result*** - It is too soon to tell. Passkeys expected early in the year are just now rolling out for mainstream users. The infrastructure to deliver passkeys is now in place. However, businesses that offer online access have to make the necessary changes to their systems to accept passkeys before individuals can adopt the tech. Large organizations like Google, Amazon, Uber and others are making passkeys the default method of logging into their services, effectively forcing adoption.
+ **Prediction #5** - Identity crimes and fraud will continue to affect generations differently. Payment and contact methods vary depending on age and how each individual interacts with the digital world.
    - » ***Result*** - Yes. There are distinct generational differences in how victims react to attacks and how they respond when victimized. Relationship scams have increased in scope and scale, with many older victims routinely reporting to the ITRC the loss of hundreds of thousands of dollars. We've never seen dollar losses as high and as often as in the past year.

- **Prediction #6** - The increased popularity of payment apps among scammers will prompt action by Congress or the Consumer Financial Protection Bureau (CFPB) to crack down on the misuse of these apps.
    - ***Result*** - Nope. Congress remains gridlocked with needed cybersecurity, privacy and identity protection legislation stuck in limbo or not even on the legislative agenda. Regulators have pressured financial institutions to take additional steps to ensure consumers know the risks of using instant transfer services, but no new rules have been adopted.
- **Prediction #7** - Despite continued evidence that data breaches are giving scammers the information they need to craft more effective phishing pitches and account takeover fraud, Congress will fail to pass a comprehensive privacy and data security law in 2023.
    - ***Result*** - See Prediction #6. Congress did not pass a comprehensive privacy law in 2023. In fact, they did not hold a single hearing on a comprehensive privacy law in the past year. However, nearly a dozen states have passed their own comprehensive privacy laws that give consumers more access and control over their personal information. That means residents of more than 39 states plus the District of Columbia and the U.S. territories do not have the benefits of comprehensive privacy and security laws.
- **Prediction #8** - The number of data breach notices that reveal less information about a compromise will continue to grow, putting more people and businesses at risk.
    - ***Result*** - Also, yes. "Not available" was the most common root cause of data breaches according to the notices tracked by the ITRC. We also gained direct evidence in 2023 that organizations are not reporting data breaches as required. In a multi-state settlement with a company breached in 2020, state Attorney Generals noted that 13,000 organizations were compromised in the supply chain attack – yet fewer than 700 data breach notices were tracked by the ITRC.

## The ITRC's 2024 Predictions

- **Prediction #1** - The risk of AI-driven identity scams that impact large numbers of people will be overstated, while the potential for targeted attacks on single or small groups of individuals will be underestimated. The availability of compromised consumer data and the use of large language models (LLMs) may result in AI-created, highly convincing "medical records" that could be submitted to insurance carriers. The greatest risk from generative AI will continue to be mis- and dis-information.
- **Prediction #2** - An unprecedented number of data breaches in 2023 by financially motivated and Nation/State threat actors will drive new levels of identity crimes in 2024, especially impersonation and synthetic identity fraud. That will cause more adoption of biometric-based identity verification (not recognition) tools to prove people are who they claim to be.
- **Prediction #3** - More states will adopt comprehensive data privacy and security laws. Congress will not.
- **Prediction #4** - Privacy concerns over the use of biometrics will overshadow the legitimate use cases. Despite the fact that there are safe and ethical uses of biometrics in the authentication and

verification space (provided they are consent-based and privacy-centric), lawmakers and the public will push back due to this lack of understanding.

+ **Prediction #5** - The emotional toll of identity crimes will continue to increase, and assistance providers will struggle to meet the emotional recovery needs of victims. Identity crime victimization is too often classified as not creating trauma for which a victim would require support, despite the fact that our latest *Consumer Impact Report* had 16 percent of respondents state they contemplated suicide as a result of victimization.