2025 PREDICTIONS

& 2024 Predictions Recap

ITRC | IDENTITY THEFT RESOURCE CENTER

2024 PREDICTIONS RECAP

PREDICTION 1 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.

> ***REALITY 1*** *We undershot. Not only did criminals use AI to improve their phishing lures, they created all sorts of documents used to file false insurance claims including death certificates, medical records, and accident reports. The number of insurance accounts compromised by stolen logins and passwords and phishing scams has grown by 85 percent (85%) since 2022 according to government reports.*

PREDICTION 2 An unprecedented number of data breaches in 2023 will drive new levels of identity crimes in 2024, especially impersonation and synthetic identity fraud. That will drive more adoption of biometric-based identity verification (not recognition) tools to prove people are who they claim to be.

> ***REALITY 2*** *Spot on in both cases. The number of people whose identities were compromised or misused grew again in 2024. Slightly more than one-third of identity crime victims said they had problems proving their identity after being attacked; 74 percent (74%) of people who were asked to verify their identities did so using a biometric.*

PREDICTION 3 More states will adopt comprehensive data privacy and security laws. Congress will not.

> ***REALITY 3*** *Nailed it. Twenty states have now adopted comprehensive state privacy and Cybersecurity laws. Partisan politics killed a bipartisan effort to pass a national privacy law despite an agreement between the House and Senate Committee leadership.*

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), law makers and the public will push back due to this lack of understanding.

> ***REALITY 4*** *It's complicated. Efforts to block biometric use by some members of Congress failed, but a majority (62%) of U.S. residents said they had serious concerns about biometric use to verify their identity. Still 90 percent (90%) of respondents in an ITRC survey said they provided a biometric when asked.*

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.

> ***REALITY 5*** *It's hard to describe this as "good" news: The number of victims who contacted the ITRC in the past year who contemplated suicide dropped for the first time in four (4) years – from 16 percent (16%) to 12 percent (12%). That's still too many people considering self-harm, along with other financial and non-financial impacts from identity crimes.*

2025 PREDICTIONS

As 2025 approaches, the outlook for victims of identity theft, cybercrime, and scams is increasingly concerning. Policy changes and resource reductions threaten to exacerbate the struggles faced by victims, leaving them with fewer avenues for support.

REDUCED VICTIM SUPPORT & LESS LAW ENFORCEMENT FOCUS WILL TRANSLATE INTO INCREASED IDENTITY CRIMES

Federal government priorities under the new administration are likely to deprioritize critical areas like identity crime prevention, cybercrime enforcement, cybersecurity regulations, and victim assistance program funding. Federal, state, and local governments, and non-governmental organizations (NGOs) that victims rely on to navigate complex fraud cases will see fewer resources allocated.

A significant reduction in law enforcement involvement in identity crime investigations is also likely. For example, the U.S. Secret Service's mission may shift away from investigating financial and cybercrimes to focus exclusively on protective duties. Well-connected and highly adaptable multi-national criminal enterprises would increase the scale and frequency of identity crimes that harm individuals and businesses alike with the absence of the Secret Service to investigate and disrupt cybercrime.

CRIMINAL FINES AND ASSET FORFEITURES EARMARKED TO HELP IDENTITY CRIME VICTIMS WILL DROP, TOO

With fewer identity crimes investigated and prosecuted, fewer fines will replenish the 40-years old Victims of Crime Act Fund (or VOCA Fund) which does not rely on taxpayer dollars. The consequences will be significant: fewer resources for service providers like the ITRC, fewer victims receiving aid, and a diminished ability to address the ripple effects of identity crimes.

THE CYBERCRIME JOB MARKET WILL BOOM

Professional cybercriminal organizations are gearing up for a hiring boom to take advantage of the power of Artificial Intelligence and the lack of enforceable cybersecurity standards in the U.S. Easy to use tools that do not require a high level of technical skill allow criminals to target organizations, looking for known and unknown software bugs that can be exploited for a ransomware or a cyberattack that leads to a data breach. Job postings seeking software testers are already appearing in job forums used by cybercriminals.

IT'S BACK TO THE FUTURE FOR FEDERAL REGULATIONS…AND THE FUTURE IS NOW FOR STATE REGULATORS

Proposed and in-force federal regulations that require organizations to report cyberattacks and data breaches are expected to be weakened or abandoned in the coming year. But, the number of states expected to adopt their own privacy and cybersecurity laws and regulations will grow beyond the current 20 states that have them. That's good news for residents of those states, but a state by state approach creates confusion for people and businesses and a system where geography determines your protections and support services. It's also a compliance burden on organizations that operate in more than one state.

SELF-REGULATION WILL MAKE A COME-BACK

Since federal government regulations will wane in the new year, look for voluntary, self-regulation to make a comeback when it comes to identity and cybersecurity. Self-regulation, where industries develop best practices and standards, was all the rage in the 1990s and 2000s. While such approaches allow for flexibility and innovation, they also lack the enforcement mechanisms and oversight of formal regulations. Without mandated requirements, sophisticated fraud enterprises will take advantage of inconsistent protections, leading to increased identity crimes and consumer distrust. Businesses will face greater reputational and financial risks due to breaches and fraud that stricter regulatory frameworks would help prevent.