# 2026 PREDICTIONS

*& 2025 Predictions Recap*

ITRC | IDENTITY THEFT RESOURCE CENTER

## 2025 PREDICTIONS RECAP

PREDICTION 1

### *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.

**ACTUAL** *Nailed it. Unfortunately.*

PREDICTION 2

### *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-year-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.

**ACTUAL** *Right again. Unfortunately.*

PREDICTION 3

### *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.

**ACTUAL** *Yes, but this wasn't a big stretch.*

PREDICTION 4

### *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. However, 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 in which geography determines your protections and support services. It's also a compliance burden on organizations that operate in more than one state.

**ACTUAL** *Yes and no. The Feds rolled back existing and proposed regulations, and there was no movement on a national data privacy and protection law. Again.*

PREDICTION 5

### *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. 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 that stricter regulatory frameworks would help prevent.

**ACTUAL** *See Prediction 4 above.*

# 2026 PREDICTIONS

As the digital landscape continues its rapid evolution, 2026 is poised to be a critical year for data privacy, cybersecurity and the fight against identity theft, fraud and scams. Emerging technologies, particularly artificial intelligence, are set to further redefine the nature of threats and the strategies to combat them.

## PREDICTION 1

### *AI-Powered Social Engineering Will Drive a Surge in Hyper-Personalized Identity Theft*

Artificial intelligence (AI) will be the primary engine behind highly sophisticated and scalable social engineering attacks. These AI-driven attacks will be tailored to individual victims, using personal data gathered from various breaches to craft convincing narratives that manipulate them into divulging sensitive information or transferring funds. This will lead to a significant increase in the success rate of identity theft and financial fraud.

#### PREDICTION 1A

#### *The 'Answer Engine' Dilemma: AI Model Collapse Will Obscure Victim Support*

A tectonic change in how we consume information, shifting from "search engines" to "answer engines", will create a critical new barrier for victims in 2026. As people increasingly rely on AI models for direct answers, it will become harder to find legitimate, up-to-date help and to distinguish accurate information from inaccurate or outdated content.

#### PREDICTION 1B

#### *Agentic AI Will Introduce New Autonomous Cyber Threats and Defenses*

With the growth of "agentic AI," autonomous AI agents capable of independent action and decision-making will introduce new approaches to cyberattacks and defenses. Malicious AI agents will autonomously probe for vulnerabilities, adapt attack methods in real-time, and execute complex, multi-stage attacks without human intervention. This will lead to a new arms race in AI-powered cybersecurity, where the speed and intelligence of defensive AI will be critical to mitigating the impact of malicious AI agents.

## PREDICTION 2

### *Synthetic Identities, the Collapse of Digital Trust, and the Rise of Fake Ads & Counterfeit Shops*

Criminals now use AI to create fake IDs, voice samples and "live" videos that fool verification systems. These synthetic identities are already being used to open accounts, apply for jobs and commit large-scale fraud. One compromised app can trigger identity fusion across all your connected services. Search results and social feeds are filled with AI-generated "stores" that vanish after taking payment. Criminals buy search ads that appear above real links – so you may click a fake version of your bank or retailer.

*TIP 1:* Only upload your ID through official apps or websites you type in yourself. Consider credit freezes and account alerts.

*TIP 2:* Skip the ad results; use bookmarks or type addresses directly. Use credit cards for purchase protection and avoid wire transfers or gift cards.

## PREDICTION 3

### *Resource Scarcity and Consumer Confusion Will Amplify Victim Harm*

As sophisticated scams and identity crimes increase, the resources available to support victims will continue to shrink, a trend already identified in 2025. Compounded by consumer confusion in a complex landscape of state-by-state regulations and fewer resources from law enforcement and support organizations, victims will be left to navigate the complex recovery process alone. This combination will lead to more severe and lasting victim harm.

## PREDICTION 4

### *The Regulatory Landscape for AI and Data Privacy Will Become a Complex Global Patchwork*

2026 will see a flurry of new and updated data privacy regulations specifically targeting the use of AI. While the European Union's AI Act and GDPR will continue to set a high bar, other countries and U.S. states will implement their own distinct AI and data privacy laws. This will create a complex and fragmented global regulatory landscape, posing significant compliance challenges for multinational corporations.

## PREDICTION 5

### *Sunset of Government Subsidies Will Trigger Wave of Sophisticated Benefit Scams*

In 2026, scammers will aggressively target individuals affected by the sunsetting of government subsidies, particularly those related to healthcare. As people search for new plans or assistance, criminals will deploy highly targeted impersonation scams, posing as government agencies or healthcare providers to steal personal information and funds.

## PREDICTION 6

### *Economic Instability Will Create an "Invisible Victim" Population*

In 2026, persistent economic pressures, such as high prices for consumer goods, housing instability and a volatile job market will dominate the focus of lawmakers, media and the public.

These immediate, front-and-center financial concerns will understandably overshadow "second-tier" issues like identity crimes. The consequence will be the creation of an "invisible victim" population.

PREDICTION 7

### *Quantum Computing Threats Will Force a Shift in Encryption Standards*

While full-scale quantum computers capable of breaking current encryption standards may not be widely available in 2026, the threat will become a pressing concern for cybersecurity strategies. Nation-states and sophisticated cybercriminal groups will actively engage in "harvest now, decrypt later" attacks, stealing and storing encrypted data with the expectation of decrypting it once quantum computing becomes viable.

PREDICTION 8

### *Biometric and Behavioral Data Will Become the New Frontier for Identity Crimes*

As traditional identity verification methods like passwords and knowledge-based answers become even less secure, the reliance on biometric and behavioral data for authentication will grow. Identity crimes will evolve to include the theft and synthetic creation of biometric and behavioral data. This will lead to new forms of impersonation fraud to bypass biometric security systems. In response, there will be a greater emphasis on multi-modal biometrics and continuous authentication based on a combination of physical and behavioral traits to create more resilient identity verification systems. Regulations will also need to adapt to address the unique privacy and security challenges posed by the collection and storage of this highly sensitive personal data.

PREDICTION 9

### *The New Digital Safety Mindset*

2026 will be the year digital self-defense becomes as normal as locking your front door. Most of life now happens inside browsers, apps and chats, which requires a new approach to protection:

- Turn on passkeys or 2FA for all key accounts.
- Add bank/payment alerts.
- Do a 15-minute browser cleanup monthly.
- Agree on a family pause-and-verify rule for any urgent request involving money or credentials.