

The Identity Theft Resource Center's® 2021 Predictions show fundamental shifts in how identity crimes are committed, what cybercriminals want, and the resources available to help victims

By Eva Casey Velasquez, President/CEO and James Lee, Chief Operating Officer, Identity Theft Resource Center

The Identity Theft Resource Center® (ITRC), a nationally recognized non-profit organization established to support victims of identity crimes and compromises, has released its 2021 predictions and trends. There are four things the ITRC expects to see in the next calendar year:

1. Key U.S. government resources dedicated to financial and identity crime victims have been eliminated. The ITRC believes options for direct assistance will continue to decline in 2021.

- o Since 2018, U.S. Department of Justice [funds allocated](#) for all crime victim services has dropped from a high of \$3.7 billion to \$1.9 billion. A vast majority of the funds have been awarded to the states to administer government offices such as prosecutors' offices and police departments.

- o Discretionary grants awarded to victim services organizations dropped from \$311 million in 2019 to \$144 million in 2020.

- o Funds to programs that support victims of financial crimes, including identity crimes and compromises, cybercrime and scams/fraud have been reduced to \$0.

2. Cybercriminals are relying less on consumers' personal information and more on consumer behaviors to commit identity-related crimes, making personal information less valuable and attractive to cybercriminals. The ITRC believes this could be a long-term trend.

- o Cybercriminals are making more money defrauding businesses with ransomware attacks and phishing schemes that rely on poor consumer behaviors than traditional data breaches that rely on stealing personal information.

- o As a result, data breaches are on pace to be [down by 30 percent in 2020](#) and the number of individuals impacted down more than 60 percent year-over-year.

- o Cybercriminals are focusing on cyberattacks that require logins and passwords to get access to corporate networks for ransomware or Business Email Compromise (BEC) scams. These attacks require less effort, are largely automated, the risk of getting caught is less, and the payouts are much higher than taking over an individuals' account. The average ransomware payouts for all businesses have grown from less than \$10,000 in Q3 2018 to more than \$178,000 per event by the end of Q2 2020. Large enterprises are making average ransomware payments of over \$1 million. BEC scams cost businesses more than \$1.8 billion in 2019.

3. The ITRC believes pandemic-related identity crimes will impact victims well into 2021. R e-victimization rates for identity crimes and compromises are rising, too.

- o Millions of state [unemployment benefit-related identity theft cases](#) have been detected across the country since March 2020. Victims may not be aware that unemployment benefits have been obtained using their identity credentials until they file their tax returns and discover that the IRS is penalizing them for failing to claim the fraudulent benefits as income.

o The ITRC's Aftermath survey data shows an increase in identity crime re-victimization (28 percent in 2019 versus 21 percent in 2018) occurring before the massive increase in fraud/scams and identity crimes in 2020. The post-pandemic analysis should show an even greater rise.

o [Subscribe to our data breach newsletter](#) to get our full 2020 report in late January 2021. The 2020 data breach report will expand on some of the 2021 predictions.

4. The ITRC expects privacy, cybersecurity and identity laws to continue to merge into a more holistic set of public policies – at least at the state level – as evidenced by California voters passing the Consumers Privacy Rights Act (CPRA), the toughest privacy law in the U.S.

o The European Union started the trend in 2016 with the adoption of the comprehensive General Data Protection Regulation (GDPR) that governs data, identity privacy and cybersecurity. Two U.S. states followed in 2019 and 2020 with GDPR style laws – New York and California – with more states exploring similar laws when the COVID-19 pandemic interrupted most state legislative sessions.

o California [voters approved the CPRA](#), a more comprehensive privacy and cybersecurity law that brings the state's unified approach closer to the GDPR. The CPRA adds more consumer controls over behavioral marketing and requires routine cybersecurity audits and privacy risk assessments for companies that collect and maintain consumer information.

“While we cannot predict what will happen in the future, some of the data is troubling,” said Eva Velasquez, president and CEO of the Identity Theft Resource Center. “Federal government funds for victim services continue to be reduced, and they have been eliminated for identity crime victims. That action comes at a time when fraud and cybercrime that impact consumers are growing. The number of “repeat” victims – people who have been the target of more than one identity crime or compromise – is also on the rise along with the non-financial impacts of these crimes.”

“There is a clear shift in tactics away from cyberattacks that require mass amounts of consumer information to fuel identity crimes – and that's good news for consumers. With that said,

businesses of all sizes are now the targets of cybercriminals who know how to take advantage of human behaviors – not hope for a technology failure – to rake in billions of dollars. That harms consumers, too.”

“There are clearly some headwinds to provide assistance to identity crime victims. However, just as we have been for 20 years, the ITRC will fight for those impacted by the misuse of their identity.”

Anyone can receive free support and guidance from a knowledgeable live-advisor by calling 888.400.5530 or visiting www.idtheftcenter.org to live-chat.

About the Identity Theft Resource Center®

Founded in 1999, the Identity Theft Resource Center® (ITRC) is a non-profit organization established to empower and guide consumers, victims, business and government to minimize risk and mitigate the impact of identity compromise and crime. Through public and private support, the ITRC provides no-cost victim assistance and consumer education through its call center, website, social media channels, live-chat feature and ID Theft Help app. For more information, visit: <https://www.idtheftcenter.org>

Media Contact

Identity Theft Resource Center
Alex Achten
Earned & Owned Media Specialist
888.400.5530 Ext. 3611
media@idtheftcenter.org

