The University of Texas at Austin
Center for Identity

Identity Theft Assessment and Prediction Report 2017

UTCID Report #1706

March 2017

This UT CID research was supported in part by the following organizations:

Executive Summary

Why Read the ITAP Report?

As identity theft, fraud, and abuse continue to grow in terms of both scope and impact, individuals and organizations alike demand a deeper understanding of their vulnerabilities, risks, and resulting consequences.

The Identity Threat Assessment and Prediction (ITAP) model provides unique, research-based insights into the habits and methods of identity threats, and to the various factors associated with higher levels of risk for PII compromise and abuse. ITAP uncovers the identity attributes most vulnerable to theft, assesses their importance, and determines the personally identifiable information (PII) most frequently targeted by thieves and fraudsters.

The analytical repository of ITAP offers unique insights into people, organizations, and devices across multiple domains, including financial services, consumer services, healthcare, education, defense, energy, and government. ITAP characterizes the current identity threat landscape and aims to predict future identity threats. Using a wealth of data and analytics, the ITAP delivers some concrete guidance for consumers, businesses, and government agencies on how to avoid or lessen the impact of identity theft, fraud, and abuse. Ultimately, ITAP delivers actionable knowledge grounded in analyses of past threats and countermeasures, current threats and solutions, and evidence-driven forecasts.

What is ITAP?

The ITAP model is a risk assessment tool that increases fundamental understanding of identity theft processes and patterns of threats and vulnerabilities. ITAP captures and models instances of identity crime from a variety of sources, and then aggregates this data to analyze and describe identity vulnerabilities, the value of identity attributes, and their risk of exposure.

Through the raw data collected from news stories and other sources, ITAP aims to determine the methods and resources actually used to carry out identity crimes; the vulnerabilities that were exploited; as well as the consequences of these incidents for the individual victims, for the organizations affected, and for the perpetrators themselves. The ITAP database is a large, structured, and continually growing repository of such information, with approximately 5,000 incidents captured in the model to date. The cases analyzed occurred between 2000 and 2016. A variety of analytical tools are applied to this body of information that enable Center researchers to show and compare threats, losses, and trends in the identity landscape.

Key Takeaways

Human Error Is An Important Driver Of Identity Crime

About 17% of the incidents were non-malicious incidents in which PII is compromised, but without malicious intent on the part of those responsible. Vulnerabilities caused by human error are frequently exploited by opportunistic hackers and fraudsters.

The Impact Of Identity Crime Is Overwhelmingly Local

Only 0.36% of the identity theft incidents spanned the whole U.S., such as the infamous Target Breach in 2013. That means that over 99% of the cases are confined to a local geographic region or victim profile.

Identity Crime Is Not Only About Dollars And Cents

Emotional distress experienced by the victims is involved in a higher percentage of incidents than financial and property loss. Emotional impact is consistently higher than other types of loss.

The Insider Threat Is Very Real

One third of the incidents analyzed were performed solely by insiders, employees of companies, and family members of individuals.

Identity Theft Is Not Always A Cybersecurity Problem

Over half of the instances of identity theft, fraud, and abuse captured in ITAP did not involve —or at least did not begin with— the exploitation of cyber-vulnerabilities.

Identity Crime Affects A Wide Range Of Public And Private Sectors

The top five most affected sectors are Consumer/Citizen, Healthcare and Public Health, Government Facilities, Education, and Financial Services.

PART I

Events

Amount of Non-Malicious Activity

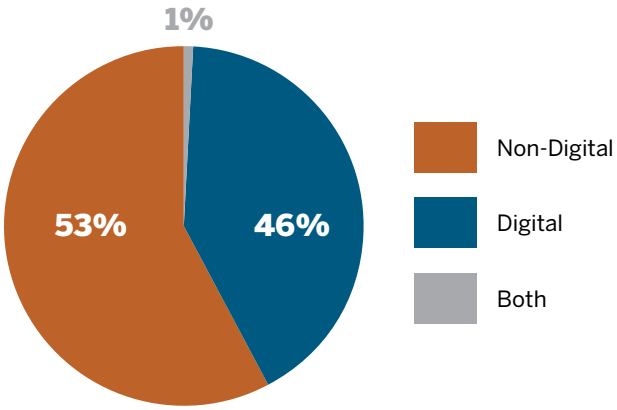
This shows the percentage of incidents categorized as non-malicious. A non-malicious incident is one in which PII is compromised, but without malicious intent on the part of those responsible for the initial compromise.

17.41%

Non-Malicious Events

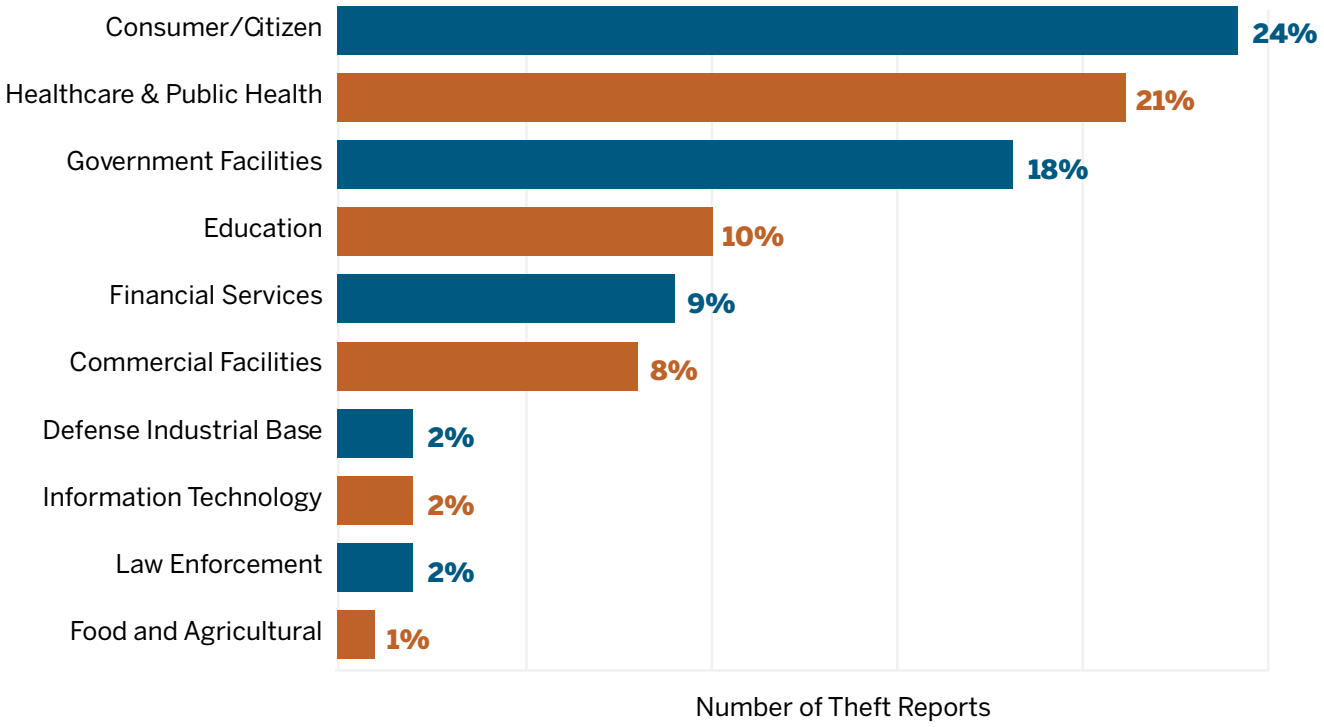
Non-Digital vs. Digital

This pie chart shows the percentages of PII theft incidents in ITAP that were “digital”, “non-digital" and both. A theft is considered purely digital if the resources used by the perpetrator(s) include nothing other than computers (or other digital devices), the internet (or other computer networks), and information accessible via such networks. A theft is purely analog if it primarily involves physical actions (beyond those required to operate a digital device); e.g. breaking into an office and stealing a laptop. An example of “both” would be a case in which the perpetrator gets someone to reveal a password over the telephone via social engineering (analog), and then uses the password on a website to access the victim’s bank account information (digital).



Market Sector

The top 10 market sectors affected by incidents of identity theft, fraud or abuse.



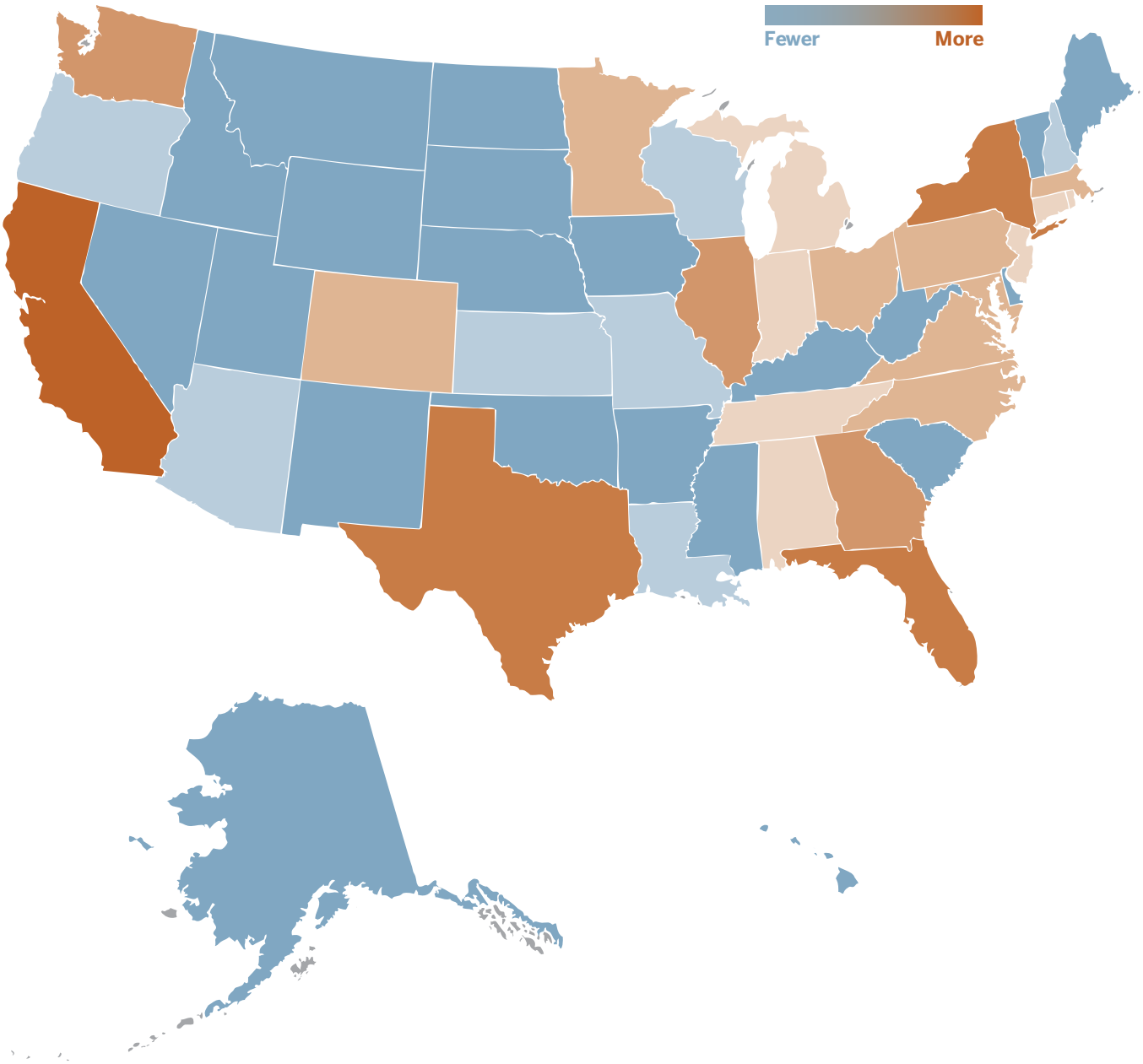
National Impact of ID Theft

This shows the percentage of incidents in which PII was compromised in the U.S. such that the incident was local to a particular city (or cities), county, state, or region. This is as opposed to incidents that have nationwide or worldwide effects.

99.64%
Localized

Number of Cases of PII Compromised in USA

This shows a six-color map of the US. The closer a state's color is to the dark brown end of the scale, the greater the number of incidents of PII compromise that have occurred in the state; while the closer a state's color is to the dark blue end of the scale, the fewer the number of such incidents that have occurred in the state. Currently, California leads with 476, followed by Florida (309), New York (303), and Texas (244).

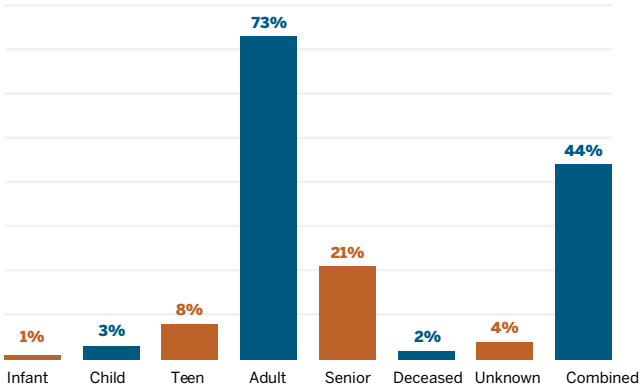


PART II

Victims

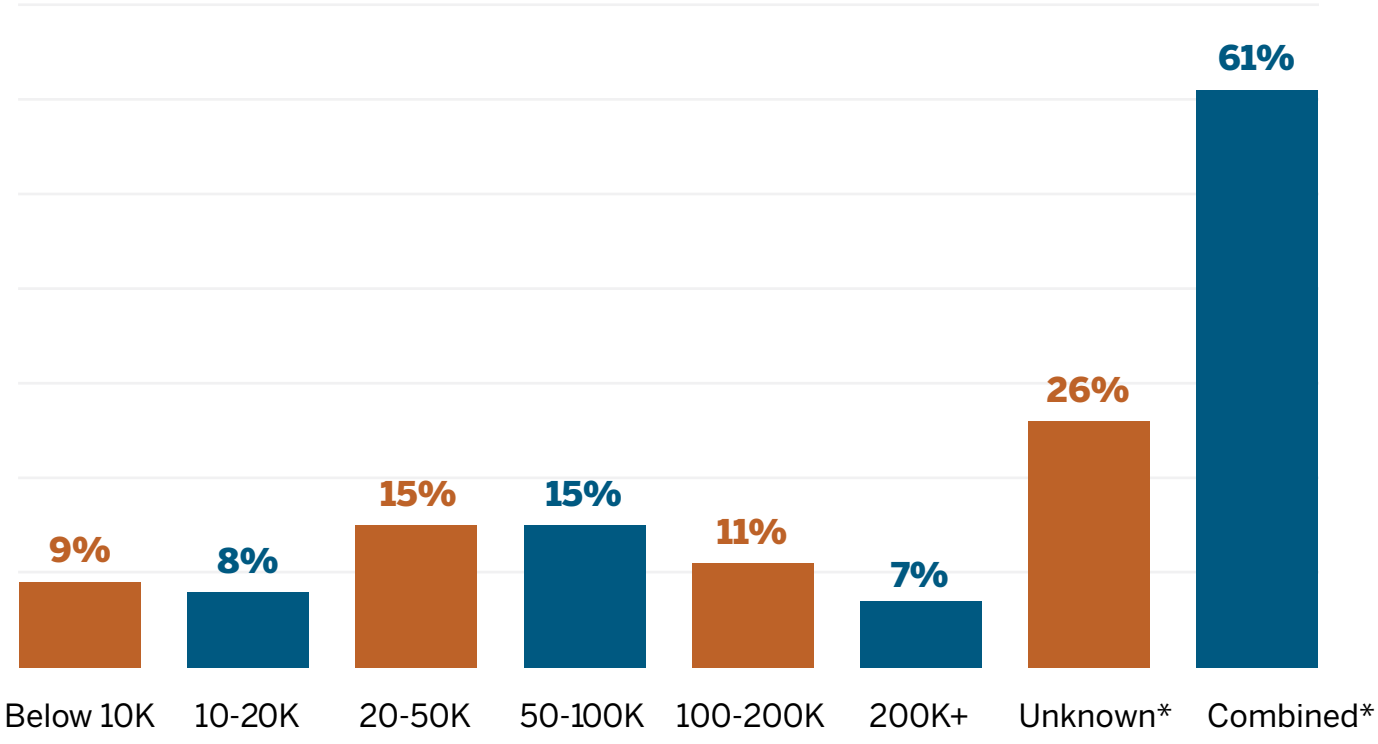
Age Group of Victims

This bar chart shows the percentages of different age groups of the victims of incidents in which PII was compromised.



Annual Income of Victims

This bar chart shows the percentages of different income levels of the victims of incidents in which PII was compromised.

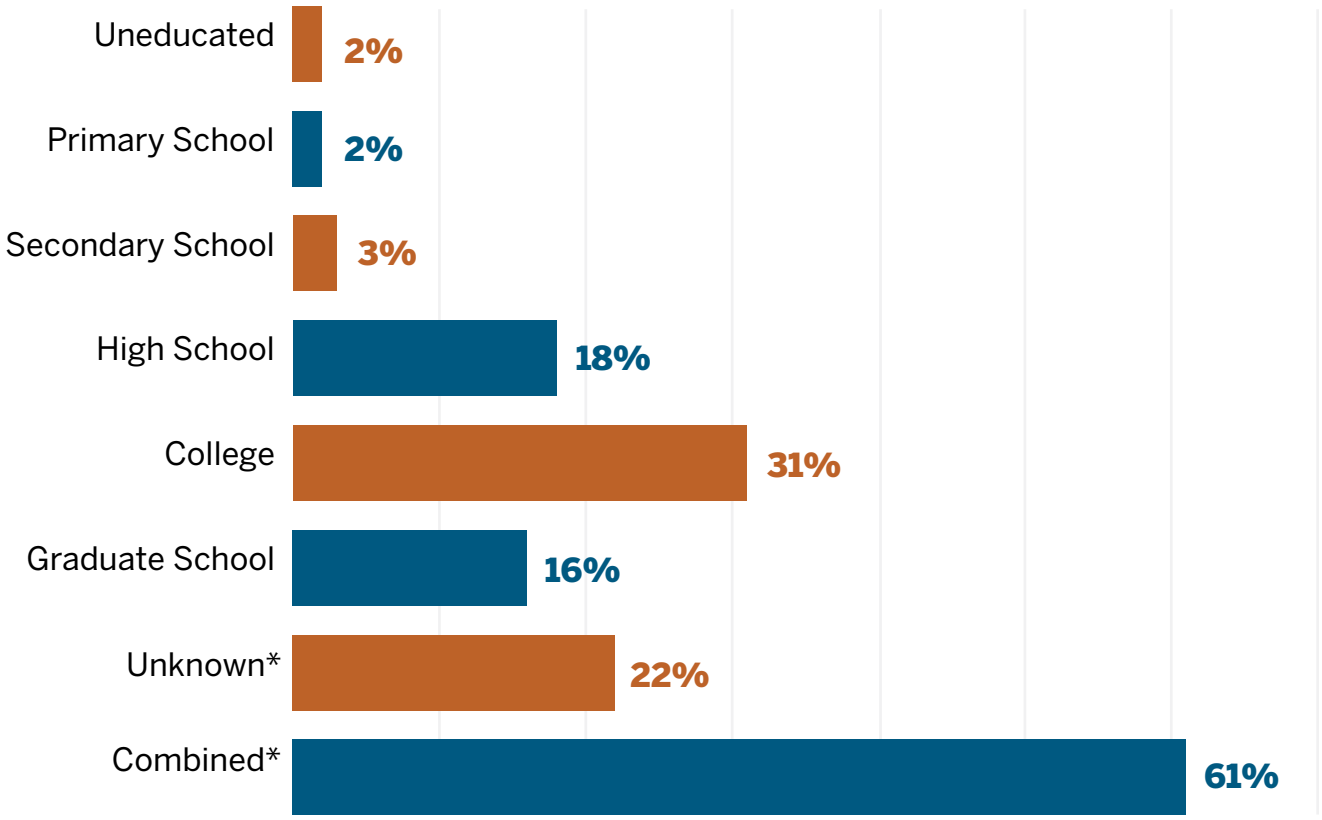


*Many cases involved victims from more than one category, so that values add up to more than 100%.

*Uknown indicates cases where no specific value for Age or Annual Income of victims can be inferred based on available case data.

Education Level

This horizontal bar chart shows the percentages of different levels of education completed by the victims of incidents in which PII was compromised.

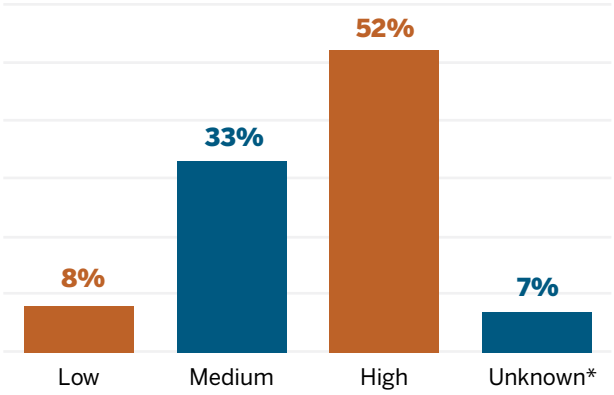


*Many cases involved victims from more than one category, so that values add up to more than 100%.

*Uknown indicates cases where no specific value for Age or Annual Income of victims can be inferred based on available case data.

Emotional Distress

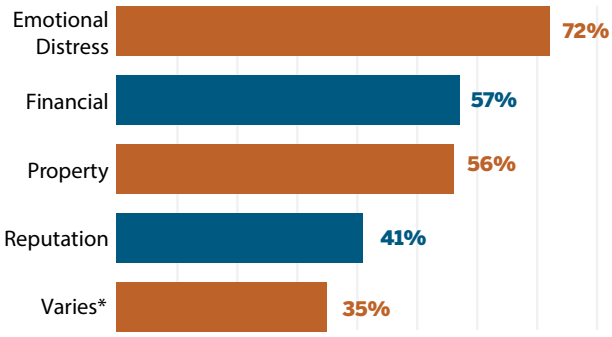
This vertical bar chart shows percentages of different levels of emotional distress experienced by the victims of incidents in which PII was compromised. The level of damage is characterized as High, Medium, Low, or Unknown. Given that our data sources generally do not provide information pertaining to emotional distress, a reasonable inference is made that the level is emotional impact is proportional to the sensitivity of PII compromised. (i.e. SSN compromise implies greater emotional impact than mailing address). The level of distress is assigned accordingly.



Level of Emotional Distress

Type of Loss

This horizontal bar chart shows the percentages of different types of loss experienced by the victims of incidents in which PII was compromised. ITAP models four types of loss: Economic Loss, Property Loss, Reputation Damage and Emotional Impact.



*Many cases involved victims from more than one category, so that values add up to more than 100%.

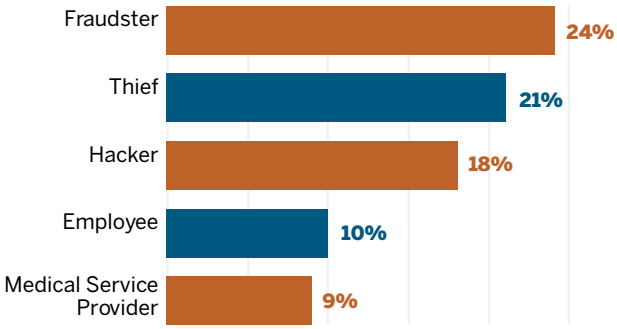
*Uknown indicates cases where no specific value for Type of Loss of victims can be inferred based on available case data.

PART III

Perpetrators

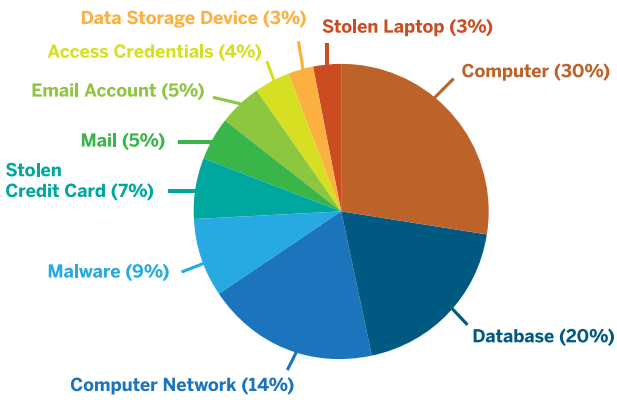
Performers

ITAP differentiates between different types of perpetrators involved in specific incidents of identity crime. So where a thief is the person actually stealing the PII, a fraudster is only involved in its subsequent abuse or commercialization, and a hacker is someone responsible for creating or exploiting a digital or computer-based vulnerability used to compromise identity assets.



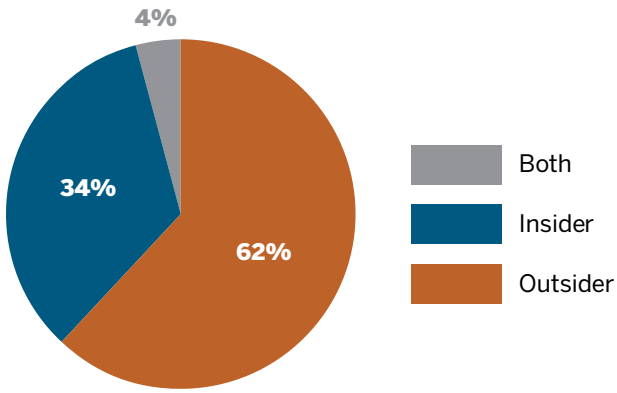
Primary Resources

This chart reflects the types of resources used by the perpetrators in each incident of theft, fraud or abuse. The top five resources used are: Computer, Database, Computer Network, Malware, and Stolen Credit Card.



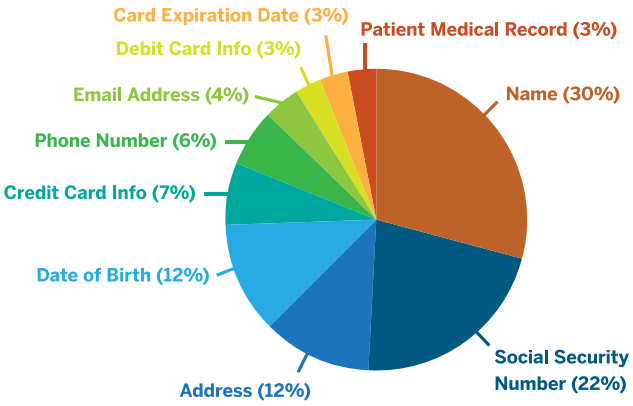
Insider vs. Outsider Activities

This pie chart shows the percentages of incidents in of PII compromise involving insiders, outsiders, and both insiders and outsiders. Insiders include employees of companies and family members of individuals.



PII Compromised

ITAP ranks PII in terms of the overall percentage of compromise. The top ten compromised PII as displayed in the image are: Name, Social Security Number, Address, Date of Birth, Credit Card Information, Phone Number, Email Address, Debit Card Info, Card Expiration Date, and Patient Medical Records.



Financial Loss Per Attribute

The average financial loss associated with a given attribute or type of PII across all cases analyzed in ITAP. The top five are displayed to the right.

Magnetic Stripe
$28,909,617

ATM PIN
$24,223,391

Fake ID Card Information
$15,177,824

Financial Information
$13,722,781

Age
$11,977,044

WWW.IDENTITY.UTEXAS.EDU