The University of Texas at Austin
Center for Identity

ITAP Report 2018

UTCID Report #18-05

MAY 2018

Sponsored By

Executive Summary

Why Read the ITAP Report?

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

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

The analytical repository of ITAP offers valuable understanding of the actors, organizations, and devices involved in identity threats, 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, ITAP delivers concrete guidance for consumers, businesses, and government agencies on how to avoid or lessen the impact of identity theft, fraud, and abuse. In sum, ITAP delivers actionable knowledge grounded in analyses of past threats and countermeasures, current threats and solutions, and evidence-driven forecasts.

This report summarizes the key takeaways from the ITAP project and then shows and explains many of the charts and lists we have designed to analyze the ITAP data. It is a simple and (we think) effective presentation of the project.

What is ITAP?

ITAP is a risk assessment tool that increases fundamental understanding of identity threat processes, patterns, and vulnerabilities. ITAP captures numerous details of actual instances of identity compromise from a variety of sources, and then aggregates and analyzes this data to recognize identity-related vulnerabilities, the values of identity attributes, and their risks of exposure or misuse.

Using 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; the types of PII that were exposed or stolen or abused; as well as the consequences of these incidents for the individual victims, for the organizations affected, and for the perpetrators themselves.

The ITAP model is a large, structured, and continually growing repository of such information, with over 5,400 incidents captured to date. The cases analyzed occurred between the year 2000 and the present. A variety of analytical tools are applied to this body of information to enable Center for Identity researchers to show and compare threats, losses, and trends in the identity landscape.

ITAP makes use of a number of fundamental distinctions to help guide its analyses. For example, it groups identity threat incidents into those that are primarily digital (i.e. carried out online via computers or other digital devices), those that are primarily non-digital, and those that are both digital and non-digital. Similarly, ITAP divides the many specific kinds of PII into four general types: What You Have (e.g. driver's license or Social Security number), What You Know (e.g. mother's middle name), What You Are (e.g. fingerprints or signature), and What You Do (e.g. travel or online browsing patterns). Also, ITAP distinguishes various types of loss or harm that identity threat victims can experience: emotional distress, financial loss, reputation damage, physical property loss, and intellectual property loss.

Key Takeaways

Ten market sectors are such that over 60% of their incidents involve two or more types of loss.

Over 50% of incidents involving high emotional distress are perpetrated by insiders (e.g. employees, family members).

Emotional distress is by far the most common type of loss, applying to 75% of all incidents. (Financial loss is the next most common, at 54%.)

Half of all market sectors -- nine of them -- are such that over 45% of their incidents involve high levels of emotional distress.

Incidents involving both digital and non-digital methods have a higher average emotional impact than those involving pure digital or purely non-digital means.

Incidents perpetrated by both insiders and outsiders have a higher average emotional impact than those performed by insiders or outsiders alone.

Less than 1% of all incidents involve the compromise of “What You Do” PII (e.g. buying habits, travel patterns).

PART I

Events

Amount of Non-Malicious Activity

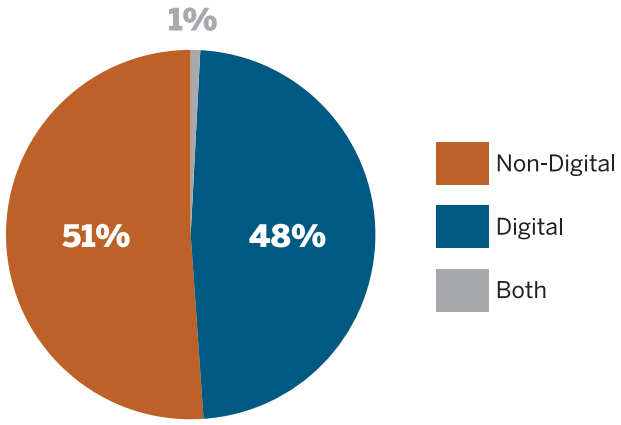
This shows the percentage of incidents categorized as non-malicious. A non-malicious incident is one in which PII is compromised, but without malicious intent on the part of those responsible for the initial compromise.

17.41%

Non-Malicious Events

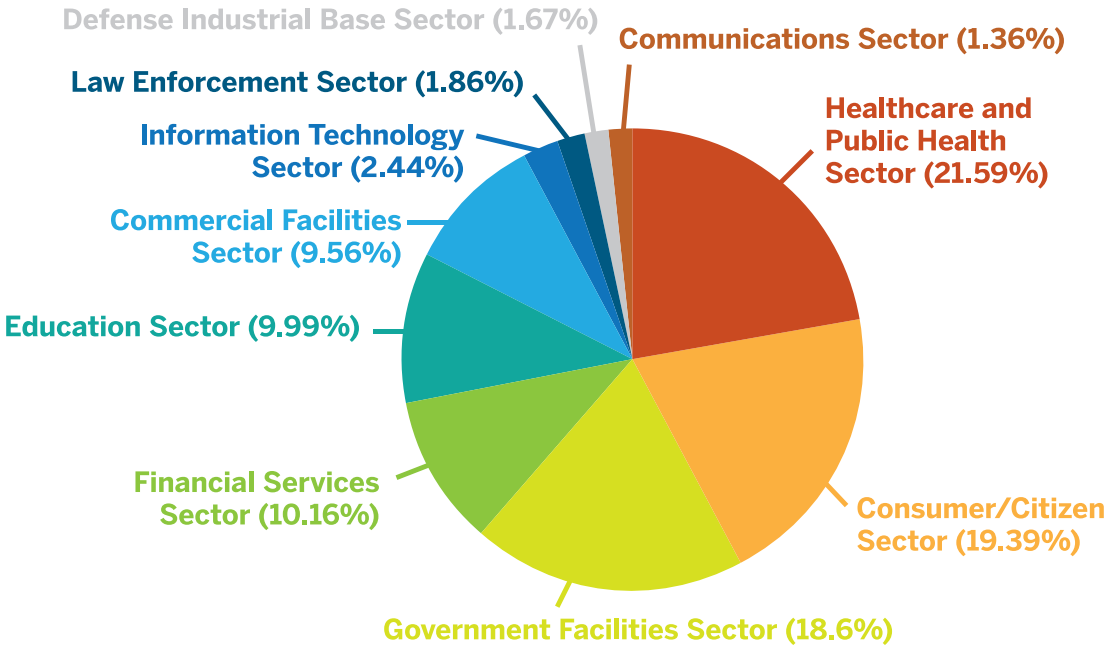
Digital vs. Non-Digital Theft

This pie chart shows the percentages of PII theft incidents in ITAP that were "digital", "analog", 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.

99.70%
Localized

*NOTE: When an incident has individual victims (as opposed to an organization) and doesn't fit into any of the other market sectors, it goes into consumer/citizen.

- E.g. one's car is broken into and their driver's license and credit cards are stolen.
- E.g. a phishing scam that targets random individuals in an attempt to steal their PII.
- E.g. someone "borrows" an older sibling's ID to get into a nightclub.

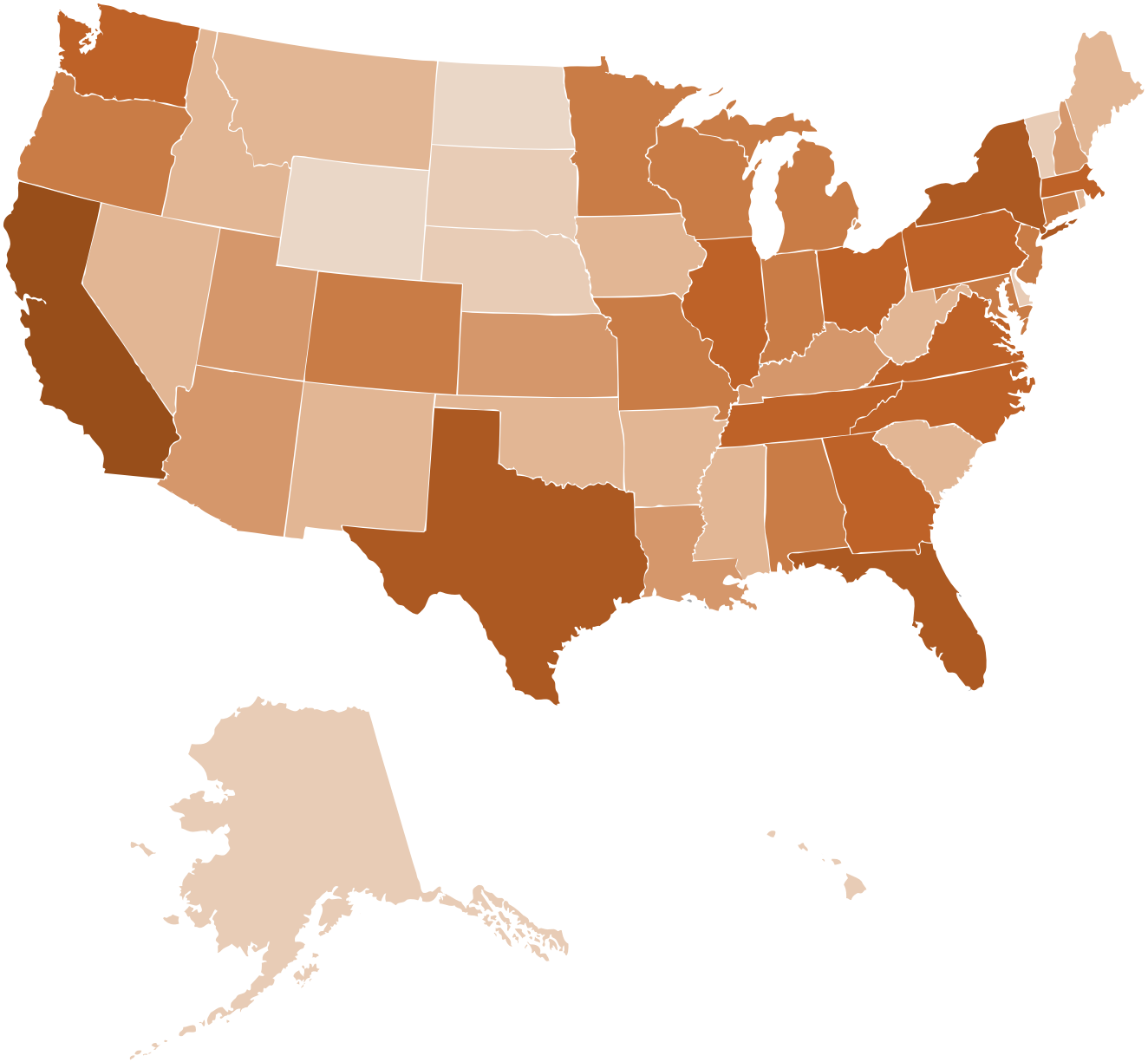
No. of Identity Thefts in the USA

This shows a six-color map of the US. The darker a state's color, the greater the number of incidents of PII-compromise that have occurred in the state. Currently, California leads with 560, followed by New York (349), Florida (358), and Texas (286).

5398

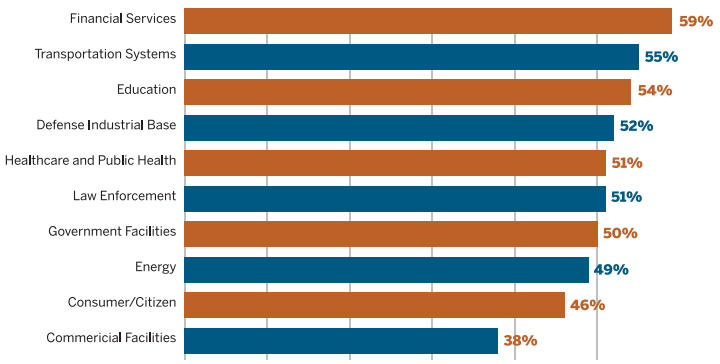
Total Number of Thefts

Fewer — More



Percentages of Incidents with High Emotional Distress—Top Sectors

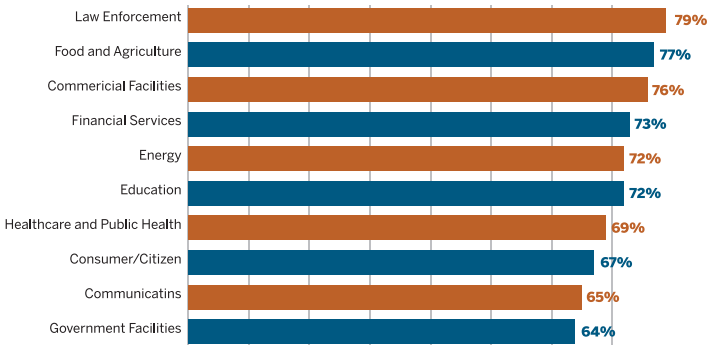
The top 10 market sectors in terms of the percentages of incidents occurring in those sectors where the victims experienced high emotional distress.



Top Sectors wrt Percentages of Incidents with High Emotional Distress

Percentages of Incidents with Two or More Types of Loss—Top Sectors

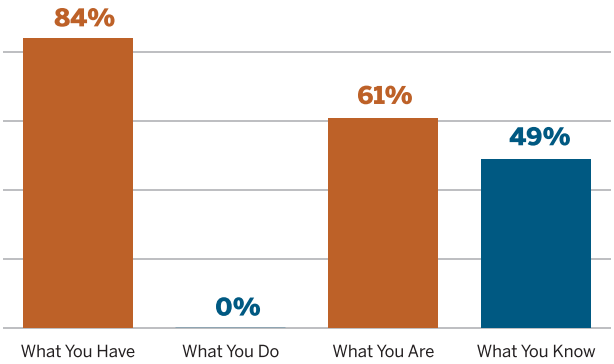
The top 10 market sectors in terms of the percentages of incidents occurring in those sectors and in which the victims suffered at least two types of loss. (The types of loss considered are: emotional distress, reputation damage, financial, physical property, and intellectual property.)



Top Sectors wrt Percentages of Incidents with two or More Types of Loss

Percentage of Incidents with PII Type Compromised

This chart shows the percentages of incidents in which each of four general types of PII was compromised. (The general types of PII considered are: What You Have, What You Know, What You Are, and What You Do.)



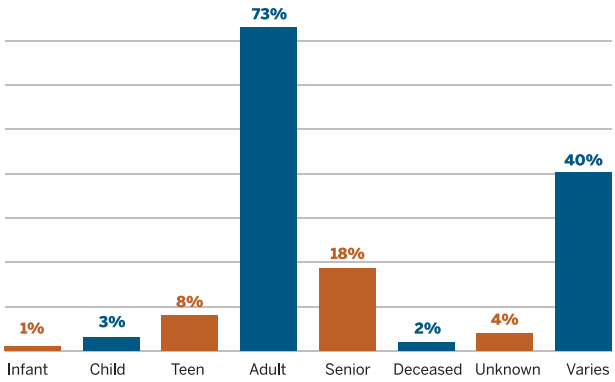
Percentage of Incidents with PII Type Compromised

PART II

Victims

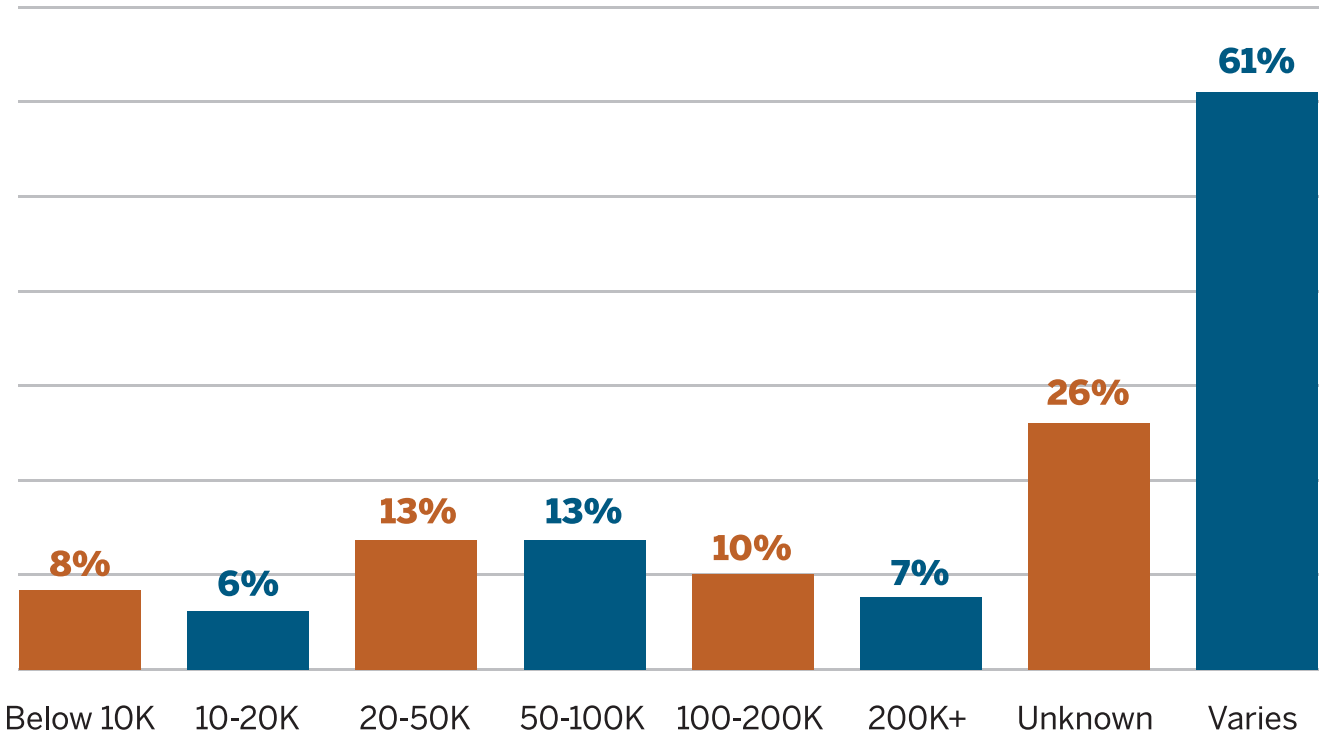
Age Group of Victims

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



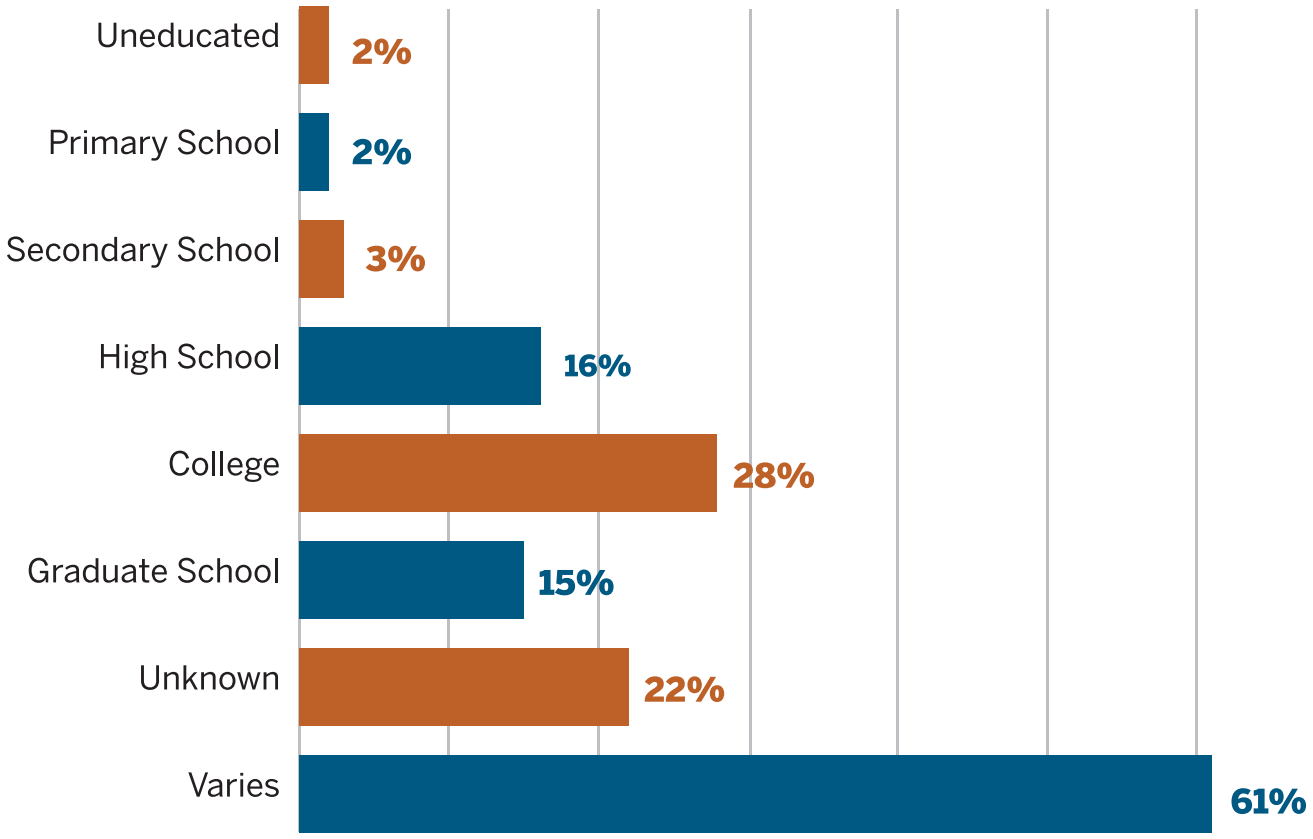
Annual Income of Victims

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



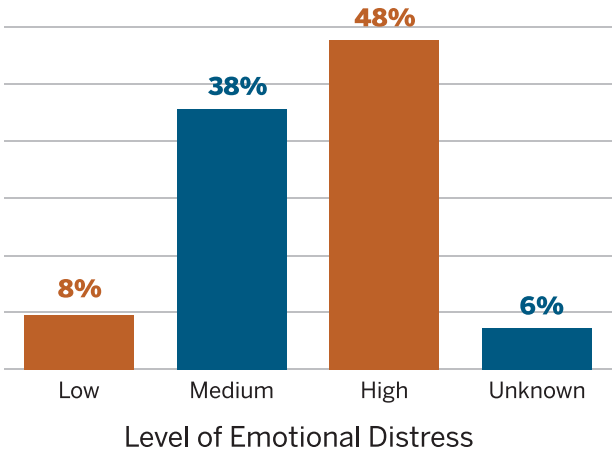
Education Level

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



Emotional Distress

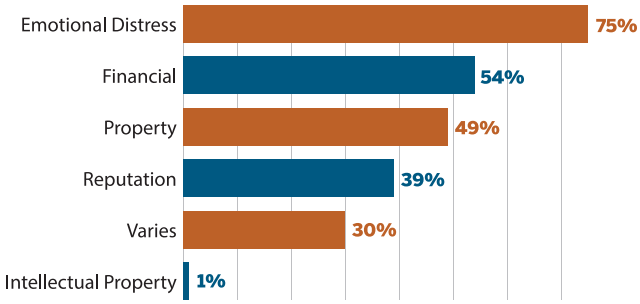
This vertical bar chart shows percentages of different levels of emotional distress experienced by the victims of incidents in which PII was compromised. The level of damage is characterized as High, Medium, Low, or Unknown.



Level of Emotional Distress

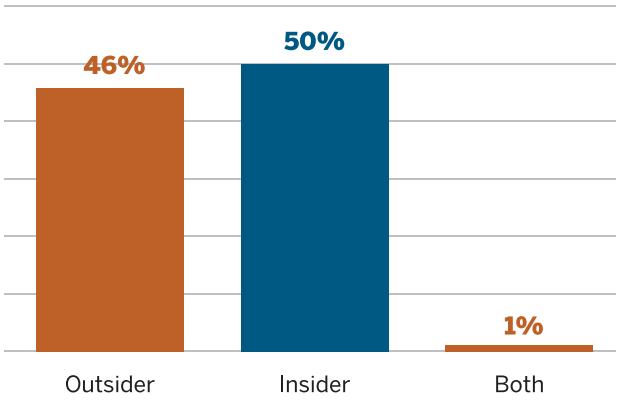
Type of Loss

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.



Emotional Impact Across Criminal Activities

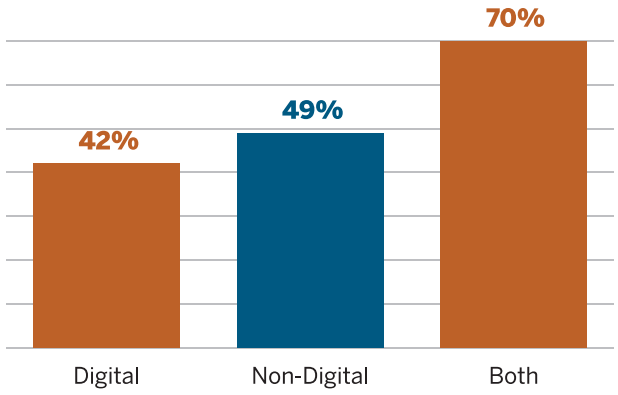
This chart shows the percentages of PII compromising incidents having a high emotional impact on the victims and where the perpetrators were (i) insiders, (ii) outsiders, and (iii) both insiders and outsiders.



Incidents with High Emotional Impact Across Criminal Activity

Emotional Impact Across Digital vs. Non-Digital

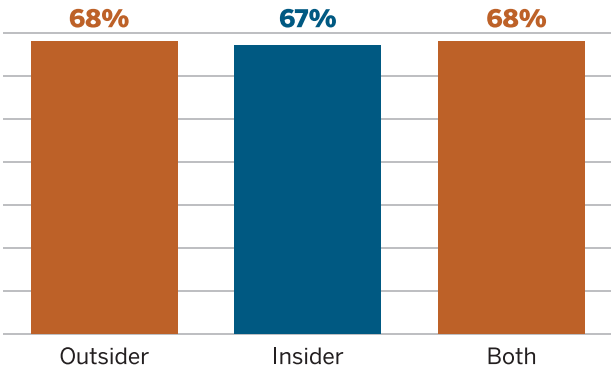
This chart shows the percentages of PII compromising incidents having a high emotional impact on the victims and where the method used by perpetrators was (i) digital, (ii) non-digital, and (iii) both digital and non-digital.



Incidents with High Emotional Impact Across Digital vs Non-Digital Theft

Two or More Types of Loss Across Criminal Activities

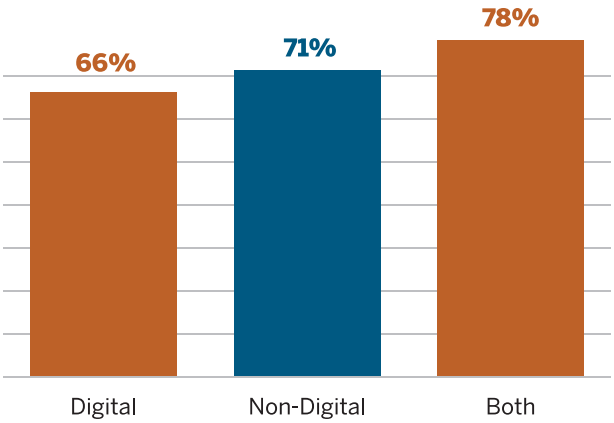
This chart shows the percentages of PII compromising incidents involving at least two types of loss and where the perpetrators were (i) insiders, (ii) outsiders, and (iii) both insiders and outsiders. (The types of loss considered are: emotional distress, reputation damage, financial, physical property, and intellectual property.)



Incidents with Two or More Types of Loss Across Criminal Activities

Two or More Types of Loss Across Digital vs. Non-Digital

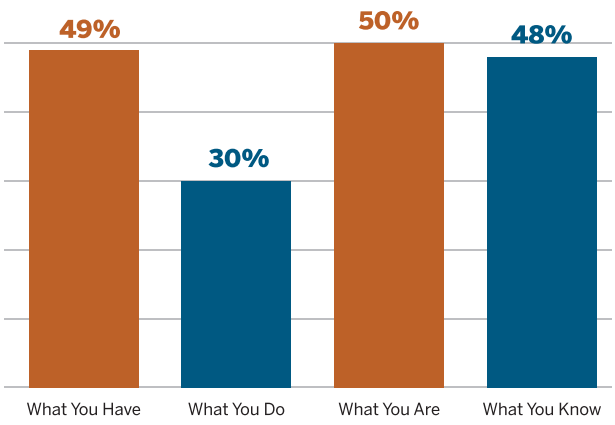
This chart shows the percentages of PII compromising incidents involving at least two types of loss and where the method used by the perpetrators was (i) digital, (ii) non-digital, and (iii) both digital and non-digital.



Incidents with Two or More Types of Loss Across Digital vs Non-Digital Theft

Incidents with High Emotional Impact with PII Type Compromised

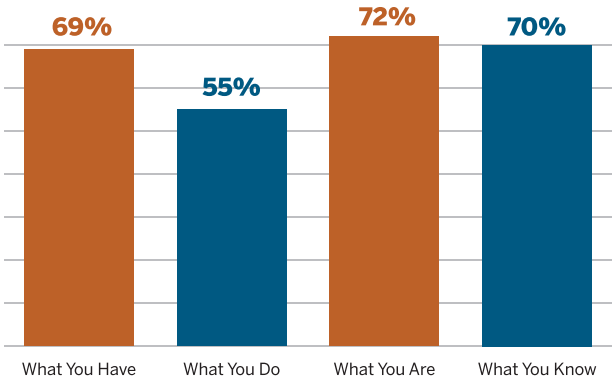
This chart shows the percentages of incidents in which each of four general types of PII was compromised and in which the victims experienced a high level of emotional distress.



Incidents with High Emotional Impact with PII Type Compromised

Incidents with Two or More Types of Loss with PII Type Compromised

This chart shows the percentages of incidents in which each of four general types of PII was compromised and in which the victims suffered at least two types of loss. (The types of loss considered are: emotional distress, reputation damage, financial, physical property, and intellectual property.)



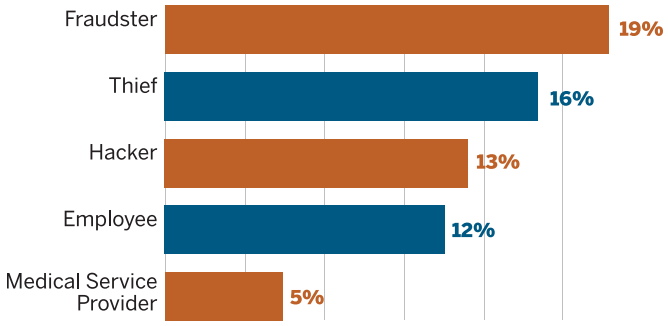
Incidents with High Emotional Impact with PII Type Compromised

PART III

Perpetrators

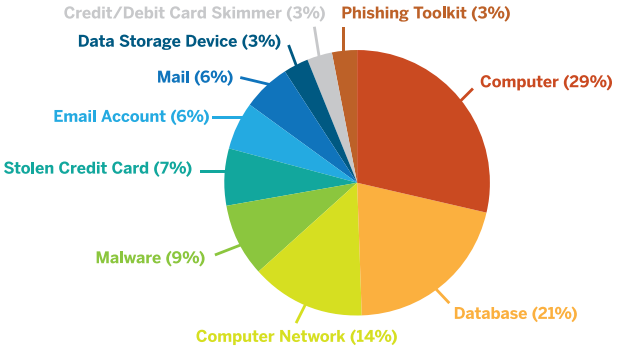
Performers

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.



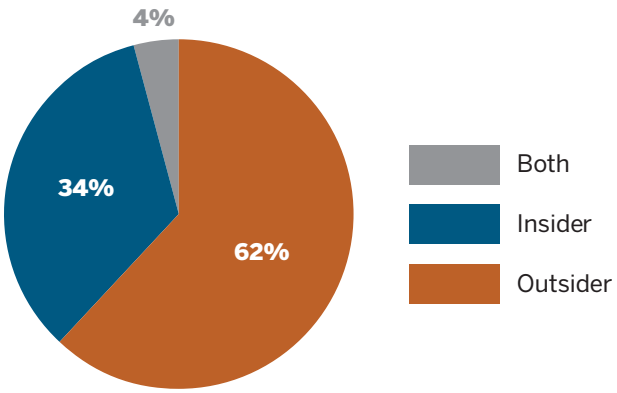
Resources

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.



Relationship of Performer(s) to Victim(s) or Organization(s)

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.



Top 5 PII Compromised in the US

This lists the top five types of PII that have most often been compromised – e.g. exposed, lost, stolen, or used fraudulently – in the U.S.

Name

 # Social Security Number

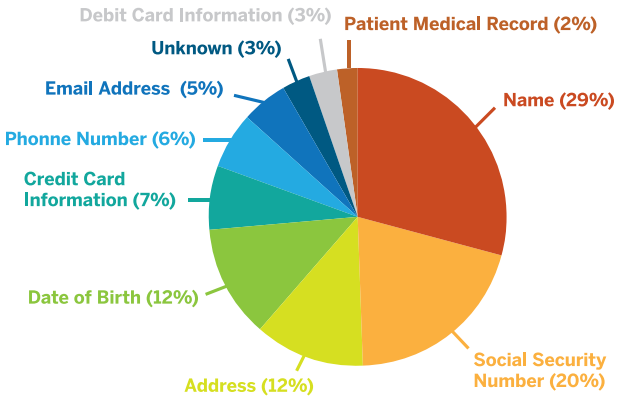
Address

Date of Birth

Credit Card Information

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, Date of Birth, Address, and Credit Card Information.



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.

Encryption Key

Fake Company Information

Fraudulent Credit Card Information

Fake ID Card Information

Debit Card Information

WWW.IDENTITY.UTEXAS.EDU