The University of Texas at Austin
Center for Identity

2019 International Identity Theft Assessment and Prediction Report

UTCID Report #19-07

JULY 2019

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

GENERALI GLOBAL ASSISTANCE
IDENTITY PROTECTION SERVICES

HID

IDEMIA
augmented identity

Symantec

TransUnion

Executive Summary

Why Read the 2019 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 own vulnerabilities and risks with respect to these threats.

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, law enforcement, communications, 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.

During 2018 and into 2019, the ITAP team focused primarily on adding international (i.e. non-US) incidents to the model. There are now about 900 international incidents captured in ITAP, making up 16% of the total number. Of the international cases, 95% were localized to a given country, while the remaining 5% were multi-national (or even worldwide) in scope. This recent focus has expanded the breadth of the project, and enabled us to implement new analytics based on international incidents, including some that compare the effects of PII-compromise across different countries. Unlike in previous annual ITAP reports, all of the charts in this 2019 ITAP Report are based purely on the international cases.

This report summarizes key takeaways from the ITAP project, with an emphasis on points of international import, and then shows and explains many of the charts and lists we have designed to analyze the international 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 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 reveal 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 captures 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 nearly 6000 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. password or 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

While we often think of cyber threats to be conducted by remote external hackers, this research finds that insider threats often take advantage of internal organizational knowledge to exploit cyber- vulnerabilities and perpetrate identity theft and fraud. An alarming 37% of these international cases involved only insiders and 8% involving both persons inside and outside the impacted organization.

Cyber vulnerabilities represent almost 75% of the cases, indicating the significant use of computers and the internet to execute these crimes.

As found in prior 2018 UT CID ITAP research investigating U.S. identity theft and fraud cases, international victims come from all income levels but victims are most often college graduates as compared to other victim educational backgrounds.

Of all the consequences and loss experienced by victims—such as financial loss, property loss, and reputation damage—it is emotional distress that is most frequently reported by victims, ranging from medium to high levels of emotional trauma.

The four international market sectors most affected by identity theft and fraud internationally match the top four most affected U.S. market sectors as reported in the 2018 UT CID ITAP Report: Healthcare, Government, Consumer Services, and Financial Services.

Many of these international cases involve three of the PII types typically found in one's wallet: "What you HAVE," "What you KNOW," and "What you ARE." "What you HAVE" credentials in particular are used in an extremely high percentage of international cases (85%) examined for this report. Over half the cases also involve "What you ARE" biometrics and "What you KNOW" biographical information.

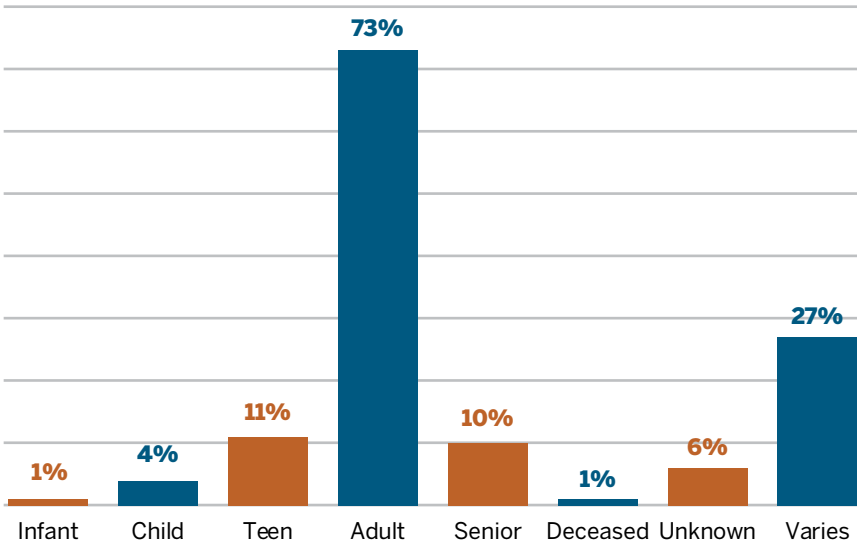
Behavioral biometrics of the type "What you DO" were involved in a relatively small percentage (5%) of the cases, but speak to an increasing amount of behavioral surveillance and consequential privacy risks.

The top 5 most frequently exposed, lost, stolen, or used fraudulently as part of the investigated cases are also some of the most public types of information.

While the globally ubiquitous internet may represent the point of entry for a large percentage of international cases, the overall impact is limited, well-defined and "local," with relatively few multi-national cases.

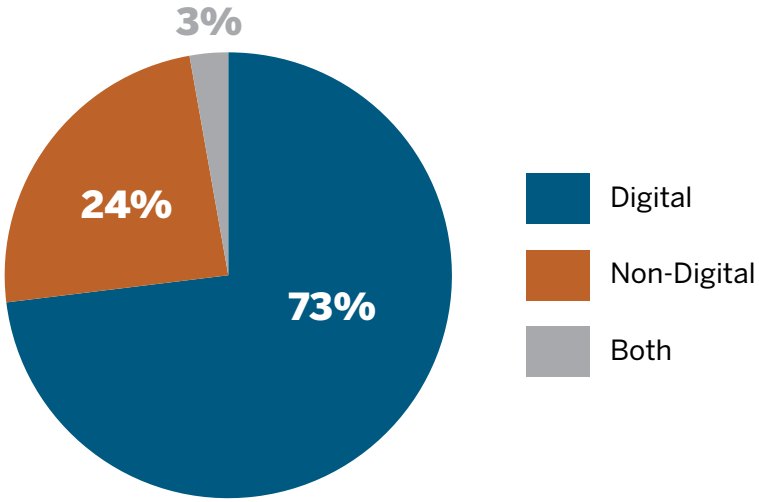
Age Group of Victims

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



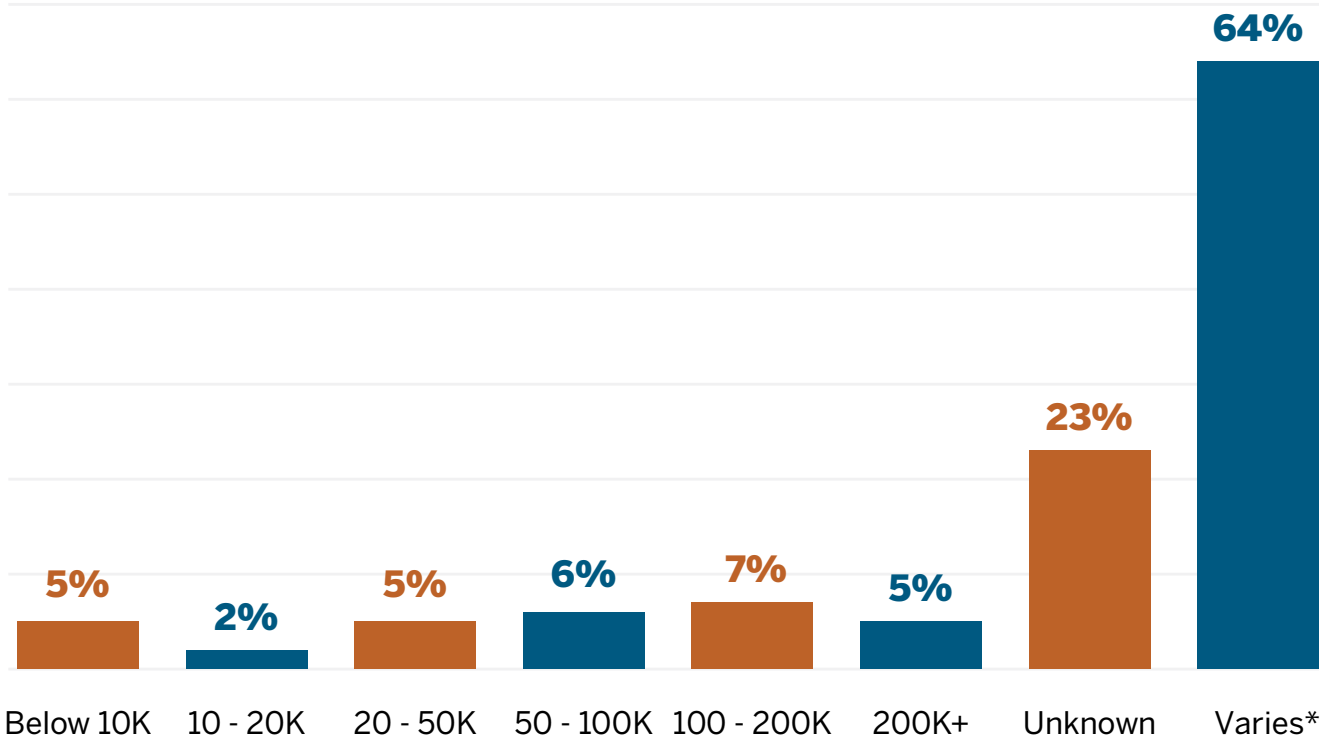
Digital vs. Non-Digital Theft

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



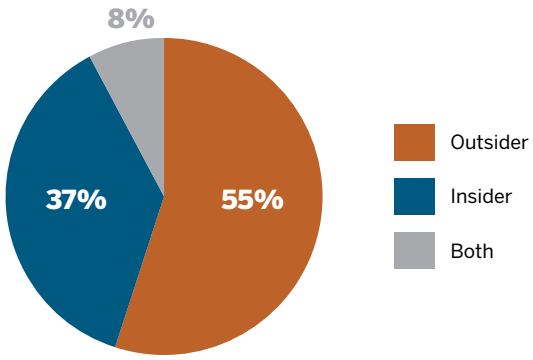
Annual Income of Victims

This bar chart shows the percentages of victims of different income levels who were affected by international incidents in which PII was compromised. (The amounts are in US dollars, calculated by the relevant exchange rate at the time of the incident.)



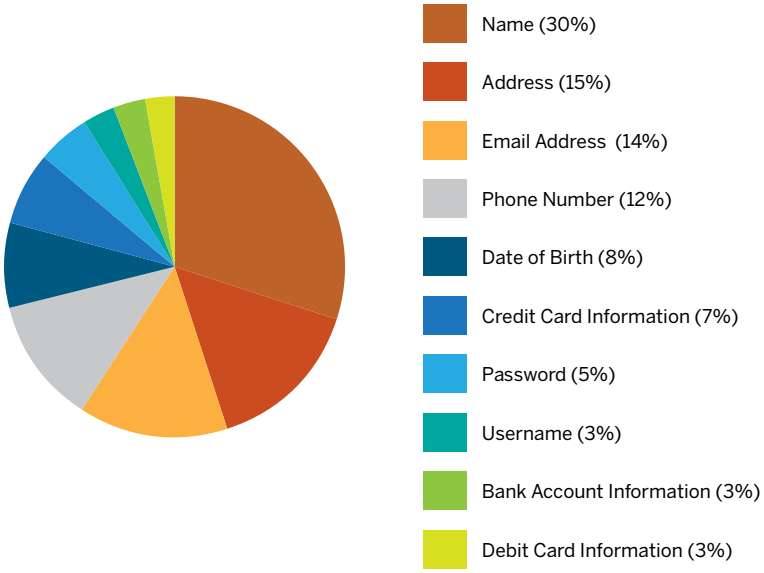
Outsiders vs. Insiders

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



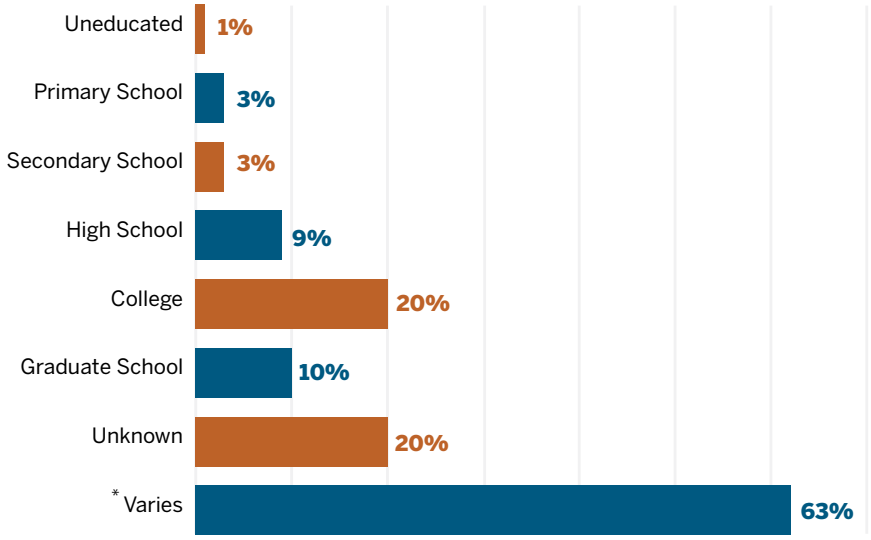
PII Compromised

ITAP ranks PII attributes by their frequency of compromise. The top ten PII attributes compromised internationally are displayed in this pie chart.



Education Level

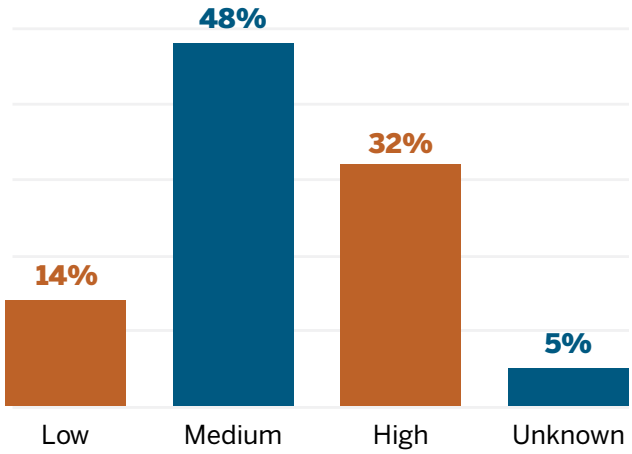
This horizontal bar chart shows the percentages of victims having different levels of education who were affected by international incidents in which PII was compromised.



*Varies indicates that a given case had multiple victims with multiple education levels

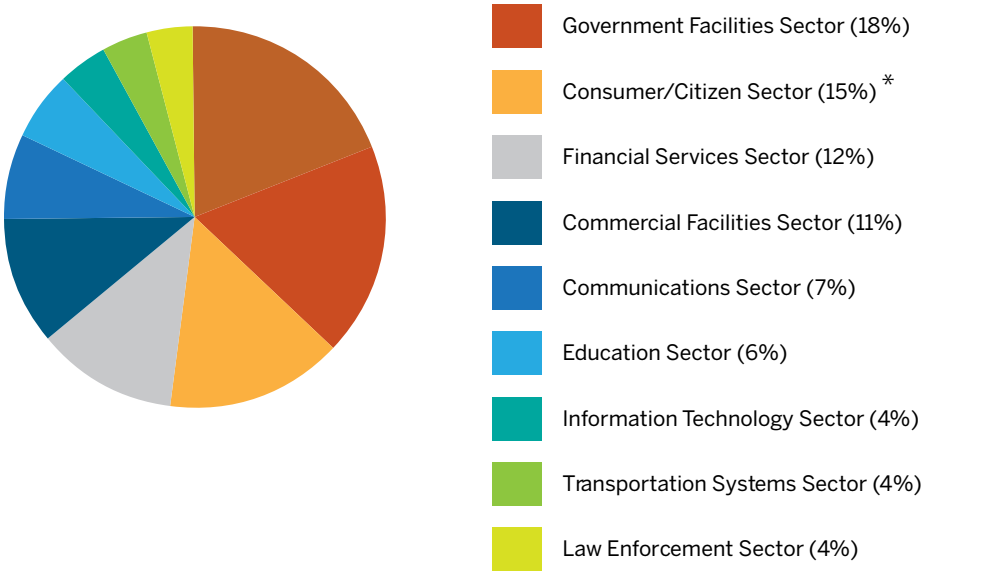
Emotional Distress

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



Market Sectors

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

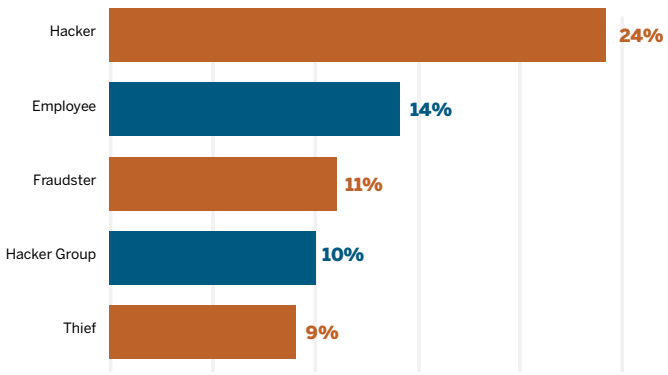


* When an incident has individual victims (as opposed to an organization victim) and doesn't fit into any of the other market sectors, it goes into Consumer/Citizen. Examples:

- Someone's car is broken into and her driver's license and credit cards are stolen.
- A phishing scam targets random individuals in an attempt to steal their PII.
- Someone "borrows" an older sibling's ID card to get into a nightclub.

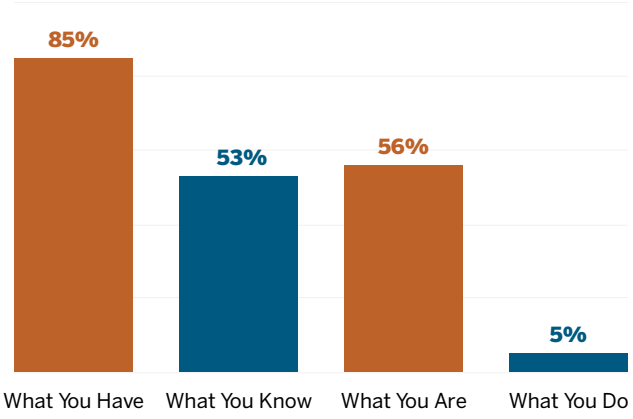
Performers

ITAP distinguishes different types of perpetrators involved in specific international incidents of identity crime. A *thief* is a person who steals PII, a *fraudster* is 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.



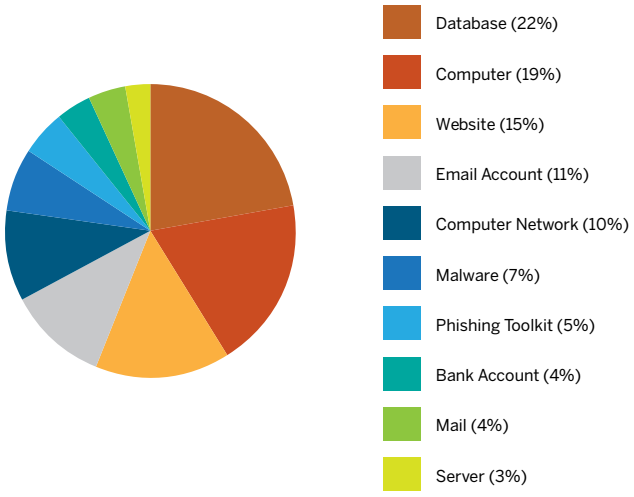
PII Types Compromised

For each of four general types of PII, this chart shows the percentage of international incidents in which some attribute of that type was compromised. The types of PII considered are: What You Have, What You Know, What You Are, and What You Do.



Resources

This chart reflects the resources used by perpetrators of international incidents of identity theft, fraud, or abuse. The top five are: Database, Computer, Website, Email Account, and Computer Network.



Top 10 Countries by Number of Incidents

This list shows the Top 10 non-US countries in terms of the number of PII compromise incidents occurring there, along with their corresponding percentages with respect to all international incidents in ITAP.

United Kingdom (22%)

Canada (21%)

Australia (11%)

India (5%)

New Zealand (3%)

Ireland (2%)

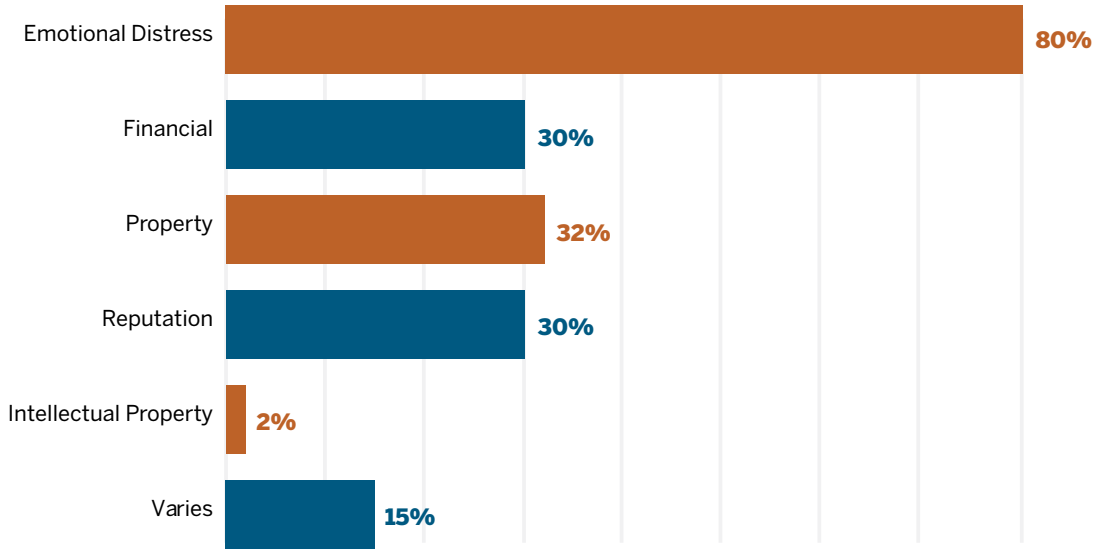
Japan (2%)

South Africa (2%)

Germany (2%)

Type of Loss

This horizontal bar chart shows the percentages of different types of loss experienced by the victims of international incidents in which PII was compromised. ITAP considers five types of loss: Emotional Distress, Financial Loss, Reputation Damage, Physical Property Loss, and Intellectual Property Loss.



Amount of Non-Malicious Activity

This shows the percentage of international 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.

28%

Non-Malicious Activity

International Impact of ID Theft

This shows the percentage of international incidents in which PII was compromised and the incident was local to a particular country or part thereof -- as opposed to international incidents that have multi-national or worldwide effects.

95%
Localized

Top 5 PII Compromised

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

- **Name**
- **Address**
- **Email Address**
- **Phone Number**
- **Date of Birth**

Financial Loss Per Attribute

We calculate the average financial loss associated with each identity-related attribute, across all international incidents in ITAP. The top five are displayed to the right.

- **Password**
- **Financial Information**
- **Date of Birth**
- **Social Security Number**
- **Photograph - Person**

WWW.IDENTITY.UTEXAS.EDU