Identity Theft Resource Center Breach Report Hits Record High in 2014
Surpasses More than 5,000 Reported Breaches and 675 Million Records Exposed Since 2005

SAN DIEGO, Calif. – January 12, 2015 – The number of U.S. data breaches tracked in 2014 hit a record high of 783 in 2014, according to a recent report released by the Identity Theft Resource Center (ITRC) and sponsored by IDT911™. This represents a substantial hike of 27.5 percent over the number of breaches reported in 2013 and a significant increase of 18.3 percent over the previous high of 662 breaches tracked in 2010. The number of U.S. data breach incidents tracked since 2005 also hit a milestone of 5,029 reported data breach incidents, involving more than 675 million estimated records.

Continuing a three-year trend, breaches in the Medical/Healthcare industry topped the *ITRC 2014 Breach List* with 42.5 percent of the breaches identified in 2014. The Business sector continued in its second place ranking with 33.0 percent of the data breach incidents, followed by the Government/Military sector at 11.7 percent. These categories were followed by the Education sector at 7.3 percent and Banking/Credit/Financial at 5.5 percent.

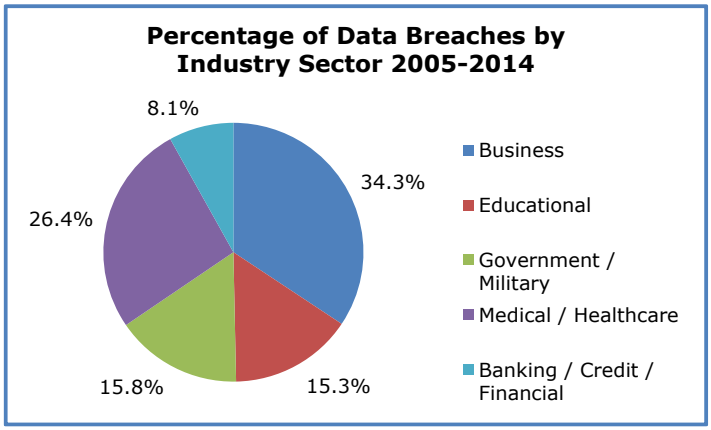
"With support from IDT911, the ITRC has been able to continue its efforts in tracking and understanding the complex issues surrounding the growing number of data breaches," said Eva Velasquez, President and CEO, ITRC. "With an average of 15 breaches a week in 2014, consumers need to be made aware of the risk of exposure to personal identifying information in order to understand the threat posed by this growing list of data breach incidents."

"The ubiquitous nature of data breaches has left some consumers and businesses in a state of fatigue and denial about the serious nature of this issue. While not all breaches will result in identity theft or other crimes, the fact that information is consistently being compromised increases the odds that individuals will have to deal with the fall out. The ITRC data breach reports are a necessary educational tool for businesses, government and advocates alike in our communication efforts," Velasquez added.

In 2014, Hacking incidents represented the leading cause of data breach incidents, accounting for 29.0 percent of the breaches tracked by the ITRC. This was followed for the second year in a row by breaches involving Subcontractor/Third Party at 15.1 percent. Accidental Exposure of information in 2014 jumped to 11.5 percent, up from 7.5 percent recorded in 2013. Data on the Move dropped to 7.9 percent from the 12.9 percent identified in 2013.

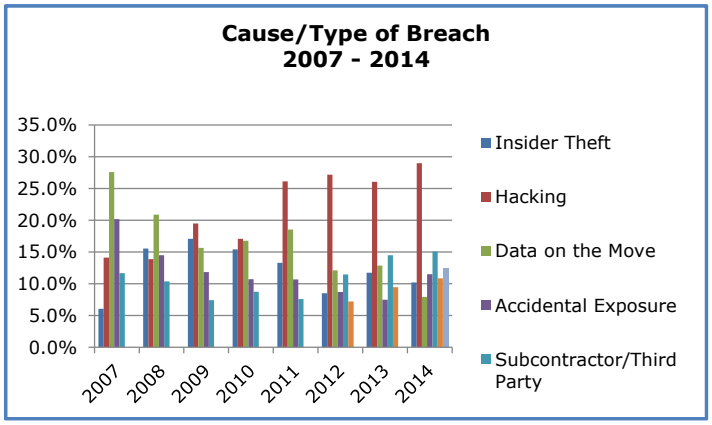
The ITRC began tracking data breaches in 2005 and since that time has been maintaining an extensive database capturing and categorizing U.S. data breaches into five industry sectors with a number of other attributes such as how information was compromised and type of data.

"It is important to note that the 5,000 breach milestone only encompasses those reported – many breaches fly under the radar each day because there are many institutions that prefer to avoid the financial dislocation, liability and loss of goodwill that comes with disclosure and notification," said Adam Levin, founder and chairman of IDT911. "Additionally, not all businesses are required to report they've had a breach for a variety of reasons, which means the number of breaches and records affected is realistically much higher."



From 2007 to 2011, the Business sector, with a 10-year average of 34.3 percent, represented the largest percentage of breaches, often far surpassing the next highest category. The Medical/Healthcare sector, with a 10-year average of 26.4 percent, took over the top spot in 2012, attributed primarily to the mandatory reporting requirement for healthcare breaches being reported to the Department of Health and Human Services (HHS). In 2005, this category reported the least number of breaches.

In 2005 and 2006, Education and Government/Military held the spots for most breaches, at 47.8 percent and 30.8 percent respectively. As indicated in the above chart, these two categories now represent a 10-year average of 15.3 percent and 15.8 percent. The Banking/Credit/Financial industry, with a 10-year average of 8.1 percent, has reported the least number of breaches for nine of the past 10 years.

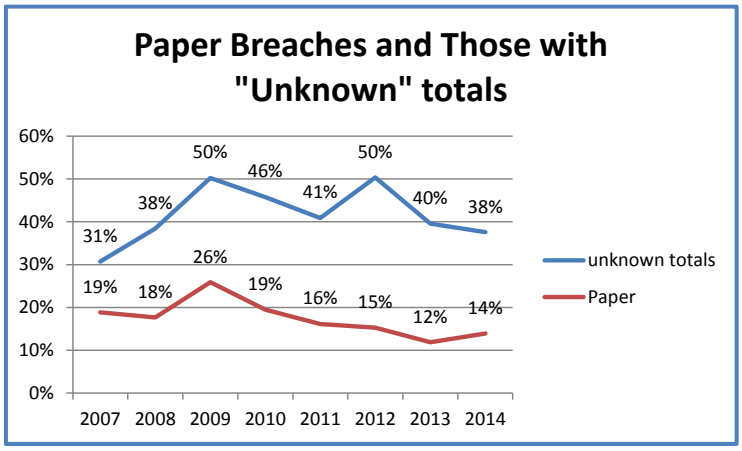


Over the years, hacking has been a primary cause of data breach incidents, leading to an 8-year average of 21.7 percent. Data on the Move, a leading cause of breaches in 2007 and 2008, ranks second with an average of 15.9 percent. (This category includes storage devices or laptops lost in transit.) Insider theft and Accidental Exposure follow at just over 12 percent, and Subcontractor/Third Party follows at 11.2 percent.

"Without a doubt, 2015 will see more massive takedowns, hacks, and exposure of sensitive personal information like we have witnessed in years past," said Levin. "Medical data and business information like intellectual property will be prime targets, with cyber

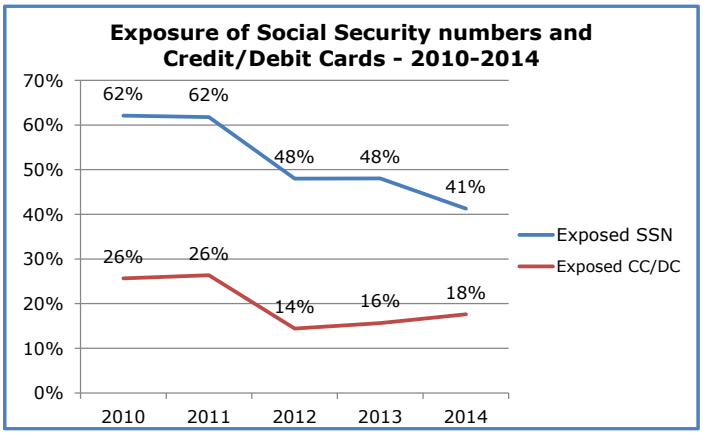
thieves looking for opportunistic financial gain based on black market value, corporate extortion and cyber terrorism."

As indicated in the chart above, other categories have been added to the ITRC database over the years. Employee Negligence was added in 2012 (3-year average = 9.5 percent) and Physical Theft was added in 2014 (12.5 percent of 2014 breaches). An eight-year average of 29.6 percent of all breaches, reported on and tracked by the ITRC, did not have sufficient information to identify the cause.



The ITRC continues to track paper breaches even though these types of breaches seldom trigger state breach notification laws. This type of occurrence has dropped considerably since the high of 26 percent recorded in 2009, with an 8-year average of 17.1 percent.

It is also noteworthy that the reporting of "Unknown", for the total number of records exposed on the ITRC Breach List, has shown a decline since the high of 50.3 percent in 2012. This again may be due to the high percentage of medical/healthcare entities which are required to report the number of records. The eight-year average of "unknown" is 41.5 percent.



Tracking of breaches involving Social Security numbers and Credit Card/Debit Card information began in 2010. The exposure of SSN's has shown a definite decline over the past five years since the high in 2010 of 62.1 percent. The same cannot be said for credit/debit cards, which reflected a rise in both 2013 and 2014. The five-year averages for these two categories are 51.3 percent and 19.8 percent respectively.

"I would love to report that the decline in breaches exposing SSNs is a testament to increased security efforts by institutions to protect the golden ticket to a consumer's identity," continued Levin. "Unfortunately, those compromises have been dwarfed by the alarming and exponential rise in successful attacks on point-of-sale systems at big box retailers. The FBI estimates that more than 1,000 retailers are under assault with the same (or tweaked versions) of the malware that compromised Target and Home Depot."

He concludes, "therefore, it is incumbent on consumers to be their own best guardian by controlling what personal information they make available in order to minimize their risk of exposure, monitoring their accounts daily so they know as quickly as possible they have an issue, and having a damage control program to help them get through identity related problems quickly, efficiently and thoroughly."

For 10 years, the ITRC has been committed to dedicating resources to providing the most accurate review and analysis of U.S. data breach incidents. This has long involved adding new categories and updating methodologies to best capture patterns and any new trends.

"Maintaining a quality multi-year data breach incident database necessitates constant attention to what is happening in the world of data breaches, legislative efforts on breach notification and industry reactions to incident response preparedness," said Karen Barney, ITRC data breach analyst. "As a credible and thorough resource, the ITRC is able to provide unique insight and information to consumers and businesses alike."

About the ITRC Breach List

The ITRC Breach List is a compilation of data breaches confirmed by various media sources and/or notification lists from state governmental agencies. Breaches on this list typically have exposed information that could potentially lead to identity theft, including Social Security numbers, financial account information, driver's license numbers and medical information. This data breach information, and available statistics, have become a valuable resource for media, businesses and consumers looking to become more informed on the need for best practices, privacy and security measures in all areas – both personal and professional.

About the ITRC

Founded in 1999, the Identity Theft Resource Center® (ITRC) is a nationally recognized non-profit organization which provides victim assistance and consumer education through its toll-free call center, website and highly visible social media efforts. It is the mission of the ITRC to: provide best-in-class victim assistance at no charge to consumers throughout the United States; educate consumers, corporations, government agencies, and other organizations on best practices for fraud and identity theft detection, reduction and mitigation; and, serve as a relevant national resource on consumer issues related to cybersecurity, data breaches, social media, fraud, scams, and other issues. Visit http://www.idtheftcenter.org. Victims may contact the ITRC at 888-400-5530.

About IDT911™ (IDentity Theft 911®)

Founded in 2003, IDT911™ is the nation's premier consultative provider of identity and data risk management, resolution and education services. The company serves 17.5 million households across the country and provides fraud solutions for a range of organizations, including Fortune 500 companies, the country's largest insurance companies, employee benefit providers, banks and credit unions and membership

organizations. A subsidiary of IDT911, IDT911 Consulting™ provides information security and data privacy services to help businesses avert or respond to a data loss incident. Together, the companies provide preventative and breach response services to more than 770,000 businesses in the United States, Canada and the United Kingdom. IDT911 is the recipient of several awards, including the Stevie Award for Sales and Customer Service and the Phoenix Business Journal Tech Titan award for innovation in breach and fraud-fighting services. The company is the organizer of the Privacy XChange Forum, an annual conference that brings together high profile privacy thought leaders. For more information, please visit www.idt911.com, www.idt911consulting.com, www.facebook.com/idt911 and www.twitter.com/idt911.