



## ITRC BREACH METER REACHES 342, TO DATE

SAN DIEGO, June 30 /PRNewswire/ -- The Identity Theft Resource Center data breach count has reached an all-time high. Between January 1st and June 27th, the total number of data breaches recorded by the ITRC is 342, more than 69% greater than the same time period in 2007. The actual number of breaches is more than likely higher, due to underreporting, and the fact that some of the breaches reported, which affect multiple businesses, are listed as a single event. The BNY Mellon and SunGard data exposures are examples of these "multiple" events. In one case, the customers and/or employees of at least 45 "entities" were affected by a breach that the ITRC reported as a single event.

1. The ITRC breach report sub-divides and tracks all breaches into five categories. The following is a comparison of 2008 (as of June 27th) with annual totals from 2007 and 2006.

-- Business:	2008-36.8%	2007-28.9%	2006-21%
-- Educational:	2008-21.3%	2007-24.8%	2006-28%
-- Government/Military:	2008-17.0%	2007-24.6%	2006-30%
-- Health/Medical:	2008-14.9%	2007-14.6%	2006-13%
-- Banking, financial, credit:	2008-10.0%	2007-7%	2006-8%

2. In 2008, ITRC's current report reveals that 58.8% of breach events published the number of records involved, and that 39.4% of those having data exposures did not disclose the number of records potentially exposed.

3. To date, electronic data breaches account for 80.7% of breach events, and paper breaches are 19.3%.

4. ITRC further categorizes data into five types of data breach scenarios. Some breaches, due to their nature, may be counted in more than one category, and some may not be fit into any of these categories. While human error and poor data handling policies and procedures certainly played a role in the 2008 data exposures, it appears that theft of data, either by external or internal sources, is the primary way information has been compromised.

ID Analytics, the leader in on-demand intelligence, also cooperated with ITRC in its 2007 breach study, and found that 39% of data exposures in 2007 were related to missing or stolen devices. More importantly, the ID Analytics analysis showed that the "malicious intent" categories (Internal Data Theft /

Internal Hacking or Intrusion / Account Level Malicious Access / External Theft) comprised 25% of the total data exposure events. ITRC believes that this indicates an increasing awareness by thieves of the monetary value of personal identifying information

-- Insider Theft (stolen by someone inside the company):	2008-15.8%	2007-6.0%
-- Data on the Move (laptop, thumb drive, PDA, etc.):	2008-20.2%	2007-27.8%
-- Subcontractor (stolen or lost by a second party):	2008-13.5%	2007-11.4%
-- Hacking (stolen by someone outside of the company):	2008-11.7%	2007-14.1%
-- Accidental Exposure (inadvertent Internet/Web posting):	2008-15.2%	2007-20.2%

5. The Identity Theft Resource Center only included verified breaches listed in newspapers and websites such as [www.pogowasright.org](http://www.pogowasright.org) , the Maryland and New Hampshire Attorneys General breach notification lists, the Wisconsin Office of Privacy Protection, [www.attrition.org](http://www.attrition.org) , [www.breachblog.com](http://www.breachblog.com) , and various other databases. State AG listings have made public some breaches that would otherwise have been unreported. ITRC would encourage more states to publicly list all notification letters so that a more complete record of known breaches can be compiled and studied.

ITRC focuses primarily on the number of breaches, and not records exposed. In almost 40% of breach events, the number of records exposed is not reported or is not fully disclosed publicly. This means the number of affected records is incomplete, therefore misleading. The use of potentially affected records, versus the number of breaches, generally causes more concern and is exploitive. However, for a reliable and credible report, ITRC focuses upon the number and types of breaches. This is also the reason that ITRC does not list the top ten breaches of the year. To list only those who took the time to audit records and/or expose the true number of potentially affected people is inaccurate.

To view the reports used to compile this study, go to the ITRC website: "Due to length of URL, please cut and paste into browser."

[http://www.idtheftcenter.org/artman2/publish/lib\\_survey/ITRC\\_2008\\_Breach\\_List.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml)

## About the ITRC

The Identity Theft Resource Center(R) (ITRC) is a non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft. It is the on-going mission of the ITRC to assist victims, educate consumers, research identity theft and increase public and corporate awareness about this problem. Additionally, ITRC has a complete breach response program to help businesses prepare for a breach, or respond to a data exposure event. Visit [www.idtheftcenter.org](http://www.idtheftcenter.org)