C is for claims hacker

Following Are Examples of Hacker Claims

Two Guys and a Laptop Undo T.J. MAXX The TJX corporation, owners of the T.J. Maxx retail chain, were the victims of a hacker attack, which was carried out over a period of two years. Because the chain had significant gaps in their electronic security system, hackers were easily able to capture sensitive data using only a laptop computer from a car in a store parking lot. As a result, customer information, including credit cards, debit cards and driver's license numbers, was stolen from the T.J. Maxx database by hackers.

In a press release, TJX stated that the information from 45.7 million credit and debit cards, and possibly more, was stolen along with data and driver's license information for 455,000 customers. TJX is uncertain about how many customers are actually at risk because they don't know what information had been deleted, according to their security protocol, or who had access to the customer information. They expressed further uncertainty over whether or not all of their customer's files were encrypted, but noted that even encrypted files could have been decoded because the hackers had the decryption tool for the TJX encoding software.

Thus far, TJX has spent nearly $17 million cleaning up after their security breach. Others predict that the company could spend up to $4.5 billion repairing the damages. Further fallout from the hacking incident has resulted in TJX being sued by credit card processors who are paying for the credit card fraud, as well as an investigation and possible fines and lawsuits by the Federal Trade Commission.

So Much More Than a Laptop On May 3, 2007, a laptop was stolen from the home of a Department of Veteran Affairs computer analyst in Montgomery County, Maryland. The laptop had the names, birth dates, and social security numbers of every living veteran since 1975. Although the data that was taken did not have health or financial records, it did have some data on veteran's spouses and some disability ratings. While the VA doesn't believe the thieves' intention was to steal veterans' personal data, they are worried they will sell the information.

Idaho's Sen. Larry Craig, expressing concern over the theft, questioned why such sensitive information was being taken out of the office. Also weighing in were other politicians and government workers who hoped this scare will light a fire under the government to take stronger actions against identity theft. The VA is in the process of notifying the veterans of the stolen information, as well as figuring out where they misstepped in their security precautions.

Chicago Public School Board Learns a Lesson 40,000 Chicago Public School teachers were the victims when two laptops were stolen from the school board's headquarters office. The names and social security numbers of the teachers were on the laptops at the direction of the school board, who hired two consultants to download this information onto the laptops.

Commenting on the theft was an independent security consultant who said that, in his opinion, transferring social security numbers in that fashion was completely unnecessary, not to mention dangerous. After the security breach, Chicago Teachers Union president, Marilyn Stewart, met with security consultants to discuss appropriate privacy measures. As a result, Ms. Stewart recommended not using social security numbers as a means of teacher identification, as well as using more encryption and tracking software.

10/2009 Edition

BSR
PO Box 768 · Hendersonville, TN 37075
(T) 800-768-7475 · (F) 615-264-3980
www.bsrins.com

MARKEL
Ten Parkway North
Deerfield, IL 60015
847-572-6000
www.markelcorp.com