SAMPLES OF

Data Breaches

univantage
Insurance Solutions

MARCH 27, 2014

Communications Company in Salt Lake City, Utah

On March 7 it was discovered that there was an unauthorized access to employee data via the payroll vendor utilized. The personal information breached includes the employee, beneficiaries, dependents, and emergency contacts, or anyone listed in the employees' HR account with the company.

The information includes names, dates of birth, addresses, income histories, social security numbers, W-2 information, and emergency contact data and appeared to have happened between February 20, 2014 and March 3, 2014.

The FBI has been contacted and is investigating the breach. An email was sent to all those affected on March 11 with instructions on how to enroll in the company-provided credit monitoring services.

MARCH 18, 2014

A Country Store in Shelburne, Vermont

The store notified customers of a computer hack to their payment processing system, similar to reported attacks by other national retailers such as Target and Neiman Marcus.

The information compromised included names, addresses, credit or debit card numbers, expiration dates and verification codes. They believe the breach occurred between November 13, 2013 and January 6, 2014. They are unclear as to how many purchases were affected.

The company has set up AllClear ID to protect identity for 12 months at no cost to those affected.

MARCH 13, 2014

Financial Advisor in Irvine, California

On February 20, 2014 the company notified customers of a theft of back-up computer drives from a secure off-site location used as part of the company's disaster recovery plan. The drives contained names, addresses, Social Security numbers, driver's license numbers and account information.

The company is providing one year of Breach Protector credit monitoring and identity theft restoration coverage.

MARCH 4, 2014

Internal Medicine Office in Eureka, California

The office notified patients of a potential security breach. It was discovered from September 25, 2013 until around October 9, 2013 that their janitorial service was mixing paper recycling containing patient information with the regular trash vs. moving it to the locked shredding bin.

As a result, the paper containing patient information ended up in the regular trash which was picked up and disposed of by the waste management company vs. being secured in the locked bin for pick up for secure shredding.

Information that may have been in the regular trash bins could have included full names of patients, Social Security numbers, insurance plan information and medical information.

DECEMBER 20, 2013

Mortgage Company in Centennial, Colorado

A former loan officer took files from the computer systems while she was still employed. The loan officer then left the company and another mortgage company ended up with the information in late July and early August of 2013. Client names, social security numbers, credit reports, bank account information, tax information, and other sensitive information related to loan applications was taken. The information was eventually retrieved and removed from the systems of the unnamed mortgage company.

DECEMBER 20, 2013

Estate Planning Office in Camarillo, California

On Friday December 20, 2013 the owner of the firm had his home burglarized in which the firm's back-up hard drive was stolen containing customer files with sensitive personal information.

NOVEMBER 20, 2013

A Tech Company in Ogden, Utah

An unauthorized person or persons gained access to the company's systems. Customer names, credit card numbers, expiration dates, CVV security codes, mailing addresses, email addresses, and phone numbers may have been exposed. The breach was discovered on November 20.

Source: Privacy Rights Clearinghouse at privacyrights.org