

First Friday Fraud Facts+

November 7, 2014



QUESTIONS OR COMMENTS:

Chris Floyd, CPA
Financial Specialist
P.O. Box 83720
Boise, ID 83720-0011

Phone: (208) 332-8814
Fax: (208) 334-3415
E-mail: cfloyd@sco.idaho.gov

Inside this issue:

Welcome	1
What is a Data Breach?	1
Fraud Case	1
Types of Data Breaches	2
Mitigating the Risks from Data Breaches	2
How to Protect Yourself	3

The Idaho State Controller's Office distributes this newsletter as a cost-effective method of increasing awareness about ways to detect and prevent fraud, waste, and abuse in government.

Welcome to First Friday Fraud Facts+ (F4+). This edition will discuss data breaches.

WHAT IS A DATA BREACH?

A Data Breach occurs when unauthorized access is gained to the personal identifying information (PII) stored in databases of retailers, financial institutions, healthcare providers, and governments. When access to personal information is acquired, the fraudster is able to transact fraudulent activity by charging purchases, raiding bank accounts, and filing tax refunds.

A data breach can be any of the following:

- Unintended disclosure—posting sensitive information online inadvertently
- Hacking or malware—electronic entry by an unauthorized party
- Payment card fraud—fraud committed with debit or credit cards without hacking, such as a skimming machine
- Insider—someone with knowledge of the process circumvents controls
- Physical loss—paper documents lost, discarded, or stolen
- Portable device—laptops, tablets, or thumb drives lost or stolen
- Stationary device—any electronic devices not intended to be portable which are stolen or compromised¹

FRAUD CASE

One of the more memorable data breaches occurred during the 2013 holiday shopping season. Target stores experienced a serious data breach between Thanksgiving and mid-December. The personal identifying information (PII) of an estimated 70 million customers was stolen during this breach. Target indicated the stolen PII contained names, credit and debit card numbers, card expiration dates, the embedded code on the magnetic strip on the back of the cards, debit card PINs, telephone numbers, and email and mailing addresses of customers.²



Holiday sales were affected by the breach, as customers were reluctant to use their credit or debit cards at Target stores, fearing they would become a victim of the data breach. The company predicted sales for the fourth quarter would be down about 2.5 percent.

Additionally, the stock value slipped in trading after the magnitude of the data breach was announced. Target lowered their fourth-quarter earnings guidance from a range of \$1.50 to \$1.60 per share down to a range of \$1.20 to \$1.30 per share.²

TYPES OF DATA BREACHES

A report in the January/February 2012 issue of Fraud Magazine detailed the types of data breaches and rate at which each occurred. The report analyzed 2,278 data breaches and 512.3 million records which were compromised between January 2005 and December 2010, a six-year period.

The report found that 39 percent of the 2,278 breach cases were caused by internal means, either through improper protection or disposal of data, theft, hacking, or loss of data. These internal losses compromised 13 percent of the 512.3 million records.

By comparison, 56 percent of the cases were caused by actions external to the organizations. The external breaches accounted for 86 percent of the 512.3 million compromised records. Of the records, 59 percent were breached by hacking or unauthorized network entry by a non-employee.¹

Unfortunately, this underscores the message that external hackers acquire significant numbers of records when they breach the network of a large entity.

One type of data breach can affect people from all walks of life. With stolen PII, an unscrupulous person can file a federal income tax return and claim a fraudulent refund before the actual taxpayer does.

MITIGATING THE RISKS FROM DATA BREACHES

Target Stores offered free credit monitoring for one year to all customers whose data may have been compromised. However, some hackers will hold onto the PII for several years until a consumer's guard has dropped before creating fraudulent transactions. Some hackers even use data mining techniques to determine which consumers may have the deepest pockets.³

HOW TO PROTECT YOURSELF

- Write to your elected representatives asking them to pass tougher laws regarding personal identifying information (PII). Technology exists that can help protect individuals from fraudulent activity.
- File your income tax return promptly.
- Check your credit report regularly.
- Safeguard your PII; shred any outdated documents and secure those you still need.
- Eliminate PII (including birthdates) from social media and other internet sites.³

¹ "Breaking Breach Secrecy" by Robert E. Holtfreter, Fraud Magazine, January/February 2012 Vol. 27 No. 1, pages 41-50.

² Idaho Statesman "Target: Data Breach Caught up to 70M Customers" (January 10, 2014). <http://www.idahostatesman.com/2014/01/10/2966088/target-data-breach-caught-up-to.html> Accessed Jan 10, 2014.

³ Fraud of the Day. "Guest Writer: Frank Abagnale" (February 11, 2014). <http://www.fraudoftheday.com/2014/02/11/guest-writer-frank-abagnale/> Accessed May 12, 2014.

