Security Breach Notice Report

[A review of the requirements of the Financial Identity Fraud and Identity Theft Protection Act and the security breach notices received by the Department there under.]

August 3, 2011

INTRODUCTION

According to FBI statistics, identity theft is one of the nation's fastest growing crimes. Identity theft occurs when a person's personal information is stolen and used without their knowledge to commit fraud or other crimes. The latest Federal Trade Commission (FTC) Consumer Sentinel Report ranks identity theft as the number one complaint category, constituting 19% of the repository's overall complaints received in 2010. The FTC's report shows South Carolina as number 29 in the national rankings with South Carolina consumers filing 2,726 identity theft complaints.

To aid in combating identity theft, South Carolina passed the Financial Identity Fraud and Identity Theft Protection Act[1] (the Act) in 2008. While other states had certain consumer protections in place relating to identity theft, South Carolina crafted one of the most consumer-friendly and comprehensive bills of its kind in the nation. In addition to making identity theft a crime, putting restrictions on the use of social security numbers and limiting information on credit card receipts, the Act includes provisions on security freezes, credit reports, records disposal and security breaches.

This report provides a summary of the Act and an overview of the security breach notices received by the South Carolina Department of Consumer Affairs (SCDCA).

FINANCIAL IDENTITY FRAUD AND IDENTITY THEFT PROTECTION ACT

A majority of the Act became effective on December 31, 2008. The law contains rights for consumers as well as requirements for public bodies and businesses.

SECURITY FREEZE

A primary provision of the bill allows consumers to place a security freeze on their credit report, which prevents someone from accessing the report without the consumer's permission. Consumers may place a freeze on their report, including those wanting to take proactive measures to protect themselves against identity thieves. The security freeze can be "thawed" or temporarily removed for a specified time or creditor. South Carolina is one of just a few states that provide this service to all consumers, free of charge.

[1] http://www.scstatehouse.gov/sess117_2007-2008/bills/453.htm

CREDIT REPORTS

The Act provides consumers with rights in the area of credit reports that mirror those in the Federal Fair Credit Reporting Act. Consumers may dispute inaccurate or untimely information on their reports. If the information is determined inaccurate, the credit reporting agency must remove it from the report and notify anyone who accessed the report over the last six months of the mistake. If the credit reporting agency disagrees with the claim, they must supply the consumer with proof the information is accurate.

RECORDS DISPOSAL

Under the Act, businesses and public bodies must properly dispose of records containing a consumer's personal identifying information (PII). PII consists of a consumer's first name combined with their last name and unencrypted or unredacted data, including the consumer's social security number, driver's license number, financial account number or other information that would allow access to the consumer's financial accounts. These records must be disposed of "in a manner that makes it [PII] unreadable or undecipherable."

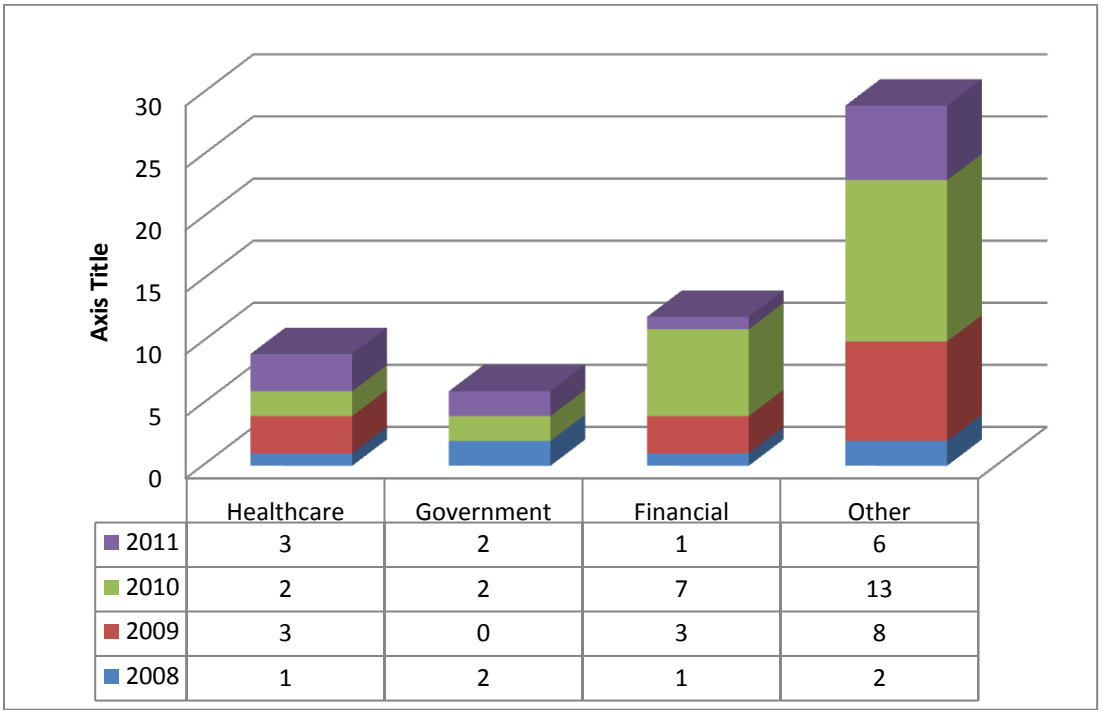
SECURITY BREACHES

State agencies and businesses who maintain personal information must alert consumers when this information may have been compromised or otherwise breached. A security breach is the unauthorized access to items containing PII when the illegal use of the PII has occurred or is likely to occur. If more than 1,000 South Carolina residents are affected by a breach at one time, the business or state agency must also notify the major credit reporting agencies and SCDCA. Security breach notices are required to contain the timing, distribution and content of the notice sent to affected consumers. This portion of the Act became effective July 1, 2009.

SECURITY BREACH NOTICES

The information provided in the following charts was gathered from notification letters sent to SCDCA by companies and governmental entities reporting security breaches from July 2008 - July 2011. While disclosures of security breaches to SCDCA were only required beginning July 1, 2009 and when affecting more than 1,000 South Carolina residents, many notifications were made out of an abundance of caution. Please be aware as you read the information provided that many companies did not report a specific number of consumers affected. Therefore, the totals provided reflect the minimum number of South Carolina residents potentially affected. During the designated time period, the Department received 56 security breach notices affecting 410, 865 South Carolina residents.

Number of Security Breach Notices Received by Industry



	Healthcare	Government	Financial	Other
2011	3	2	1	6
2010	2	2	7	13
2009	3	0	3	8
2008	1	2	1	2

Figure 1

Healthcare organizations, governmental entities, and financial service providers were the most prominent sectors reporting security breach incidents. Between July 2008 and July 2011, nine healthcare organizations, six governmental entities, and twelve financial services providers reported security breaches of consumer information. SCDCA received twenty-nine other reports from companies outside of these three main sectors. The Department received the most notices in 2010 (24) followed by 2009 (14), 2011 (12) and 2008 (6).

Number of South Carolina Residents Affected by Security Breaches

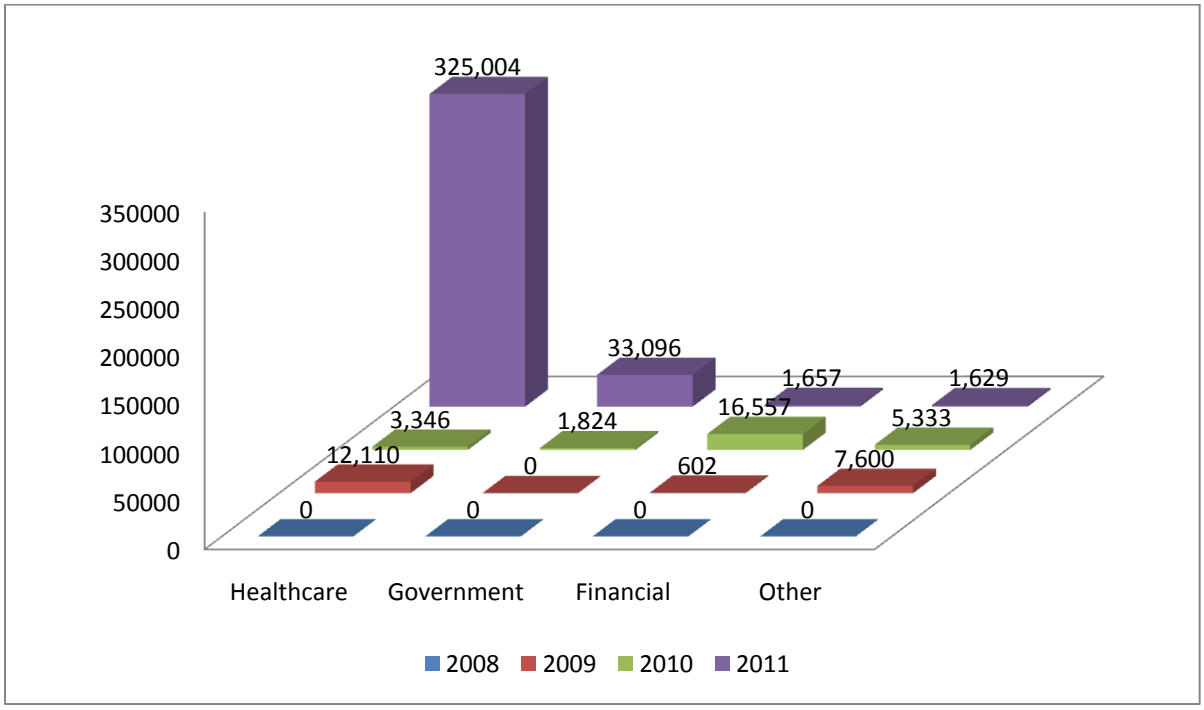


Figure 2

A total of more than 410,000 South Carolina residents were affected by security breaches of fifty-six entities. Most of the reports made during 2008 did not contain the number of consumers affected as the notice requirement had not yet gone into effect. As the notice became effective July 1, 2009, companies reported breaches affecting 20,312 consumers. This number increased to 27,060 in 2010 and rose significantly in 2011 with 361,386 affected residents.

Total Number of Notices and Affected Consumers per Industry from July 2008 – July 2011

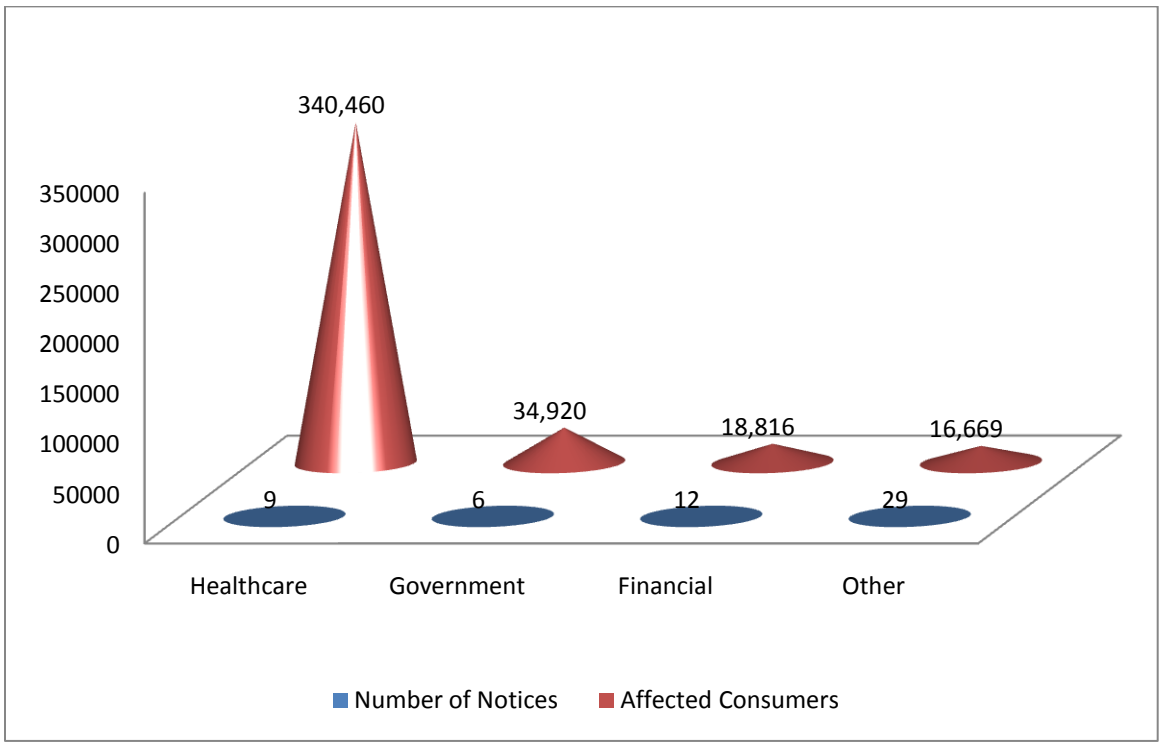


Figure 3

From 2008-2011, the healthcare industry submitted nine security breach notices that affected more than 340,000 South Carolina residents. Government notices came in second with regard to the almost 35,000 consumers affected by their six breaches. Financial organizations reported twelve breaches affecting almost 19,000 consumers while other industries filed twenty-nine notices affecting approximately 17,000 consumers.

CONCLUSION

While FIFITPA puts requirements on businesses and public bodies to protect consumers from identity theft, consumers, especially those who receive notice of a security breach, must take action to guard against this crime. Financial accounts, including bank, credit card and investment statements, should be closely monitored. Consumers also need to carefully review every "Explanation of Benefits" statement from a health insurer and request a list of benefits paid in their name on an annual basis. If incorrect or questionable information is spotted, the consumer should contact the bank or insurer immediately.

Consumers also need to check their credit reports regularly. Under federal law, every consumer has the right to receive a FREE copy of their credit report once a year from the three major credit reporting companies. To obtain a free credit report consumers can log on to www.annualcreditreport.com, call 877-322-8228, or complete the Annual Credit Report Request form found on the Federal Trade Commission Website (FTC) at www.ftc.gov/credit and mail it to Annual Credit Report Request Services, P.O. Box 105281, Atlanta GA 30348- 5281. Annualcreditreport.com is the ONLY official website offering a FREE credit report. Consumers should beware of sites, E-mails, pop-ups, and links that charge a fee for its product and services. If a consumer finds unknown activity on a credit report a dispute should be sent to the credit reporting agency, with a courtesy copy to the company reporting the information.

A security freeze is also an option that consumers can consider. This identity theft protection tool will prevent a thief from opening up new accounts in the victim's name or obtaining services where a credit report is required. Consumers are provided a password to lift or temporarily remove the freeze when needed. The freeze does not, however, guard against someone from using a stolen credit card.

For those consumers who believe they are a victim of identity theft, visit www.scconsumer.gov/publications/spotlight/Minimize_Effects_of_ID_Theft.pdf to learn how to minimize the effects. For details on what action to take in resolving specific identity theft problems see www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html . Consumers needing more information on identity theft can visit www.scconsumer.gov or call the Department toll-free at 1-800-922-1594.