insights

SHUMAKER
Shumaker, Loop & Kendrick, LLP

A Newsletter from Shumaker, Loop & Kendrick, LLP | Spring 2015

DATA BREACH:

Every Business Needs an Elite Goalie

The days of standing behind someone at the grocery store who is paying with a personal check, or, around the office, hauling physical paper files, are essentially extinct. To many Americans, the cash register and filing cabinet are now antiques. The cost-effectiveness and efficiency brought by e-commerce and digital business now saturates the U.S. and will only continue to increase with time. The rise of cloud computing infinitely expands the information landscape. The reality that critical confidential information is disseminated on a wider scale than ever before generates growing security concerns for consumers, business owners and the government.

By Michael S. Taaffe

and David L. Wyant, Jr.

Approximately two-thirds of all American adults have a smartphone. A 2014 study determined that the average American spends 162 minutes per day on their cellphone and that the average individual checks the cellphone more than 150 times per day. According to the U.S. Census Bureau, in 2013, 74 percent of all households reported Internet use. The U.S. reported over $300 billion in e-commerce in 2014, which is projected to rise by at least $50 billion this year. These figures have all grown tremendously over the last decade.

With the proliferation of employees having access to confidential and proprietary data in the increasingly commonplace American digital workplace, the security of this data in the employment context has become as crucial an issue as the one that has grabbed more headlines–the protection of consumer data in e-commerce. A staggering 94% of American jobholders are Internet users. In the workplace, employees rank the importance of Email above the Internet, landline telephone,

cellphone and social networking sites. Americans are not only connected at the workplace, but are very often also connected via electronic devices in their pockets or homes (employer-issued or not)–be it a cellphone, computer, tablet, or other Internet-capable device. In 2014, companies reported a 10% increase in "insider" incidents perpetrated by employees or former employees, solidifying such incidents as the most common of all regarding data breach.

In addition to the highly-publicized consumer data breaches occurring during the last six months at large retailers Target and Home Depot, the recent news of breaches at the second-largest health insurance company in the U.S., Anthem Inc., as well as the breaches at major financial institutions like JPMorgan, shows the compromise of millions of Americans' most sensitive information. In 2013, 19% of U.S. businesses reported losses of $50,000 to $ 1 million due to data breaches. Regardless of breach size, the American government recognizes that data security is a pressing issue.

In his 2015 State of the Union address, President Barack Obama said, "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids." The White House has taken the lead on the proposal of federal legislation to address cybersecurity and data breach. Currently there are 46 states (and the District of Columbia) that have data breach notification statutes. The hodgepodge of state notification laws creates uncertainty, which spurs the proposal of federal legislation to clear up the differences and create a national standard. The White House's proposal includes a 30-day from discovery of a breach notification requirement, and the Federal IT budget recently requested $14 billion for cybersecurity. In addition to the notification requirement, the White House will also unveil a "Consumer Bill of Rights" and will support the Federal Trade Commission in its development of a resource for victims of identity theft.

Many of the state data breach notification laws have been passed in the last few years. By the very nature of the laws' recent establishment and unseasoned enforcement, consumers and business owners are still uncertain as to how the laws work and whether they provide adequate protection. Initially there is considerable bipartisan support in Congress for federal cybersecurity regulations. In fact, several bills have been proposed in past legislative sessions. Regardless of whether Congress continues to make cybersecurity a top policy issue for the current legislative session, the safety of confidential information has never been more of a nationwide concern.

By way of example, in 2014 Florida passed its version of data breach notification laws called the Florida Information Protection Act ("FIPA"). FIPA requires that all companies take reasonable measures to protect personal data, such as encrypting it or removing personally identifiable information. Any data breach that affects 500 or more individuals must be reported to the Florida Department of Legal Affairs within 30 days, and companies must also supply forensic reports and their internal breach policies. In many circumstances, individuals whose information is compromised must also be notified by the company within 30 days. If the breach involves more than 1,000 individuals, all credit reporting agencies must be informed. There are serious consequences for failure to comply with the new rules, as companies may face fines of up to $500,000.

It is likely that both the federal government and the states that have recently implemented data breach notification laws will look to states such as California (2002), where laws have been in place for a considerable length of time as a model for effectiveness and enforcement. In light of the varying state regulations, the concept of a uniform federal law governing data breach notification and enforcement is sensible. If written with careful consideration, a federal standard could remedy the current pitfalls of the state-by-state approach, which is especially cumbersome from a compliance standpoint for nationwide businesses. Regardless, this area of the law is building momentum out of necessity and can no longer be overlooked by consumers, business owners and legal practitioners.

The Data Breach Team is led by attorney Michael S. Taaffe, who along with his team in the Sarasota office, have dealt with data breach legal issues in the financial services and other industries for many years. Other attorneys on the Team include Scott A. La Porta; Michael D. Bressan; Jarrod J. Malone; Douglas A. Cherry; David L. Wyant Jr.; and Ryan S. Nichols in the Sarasota office; Thomas P. Dillon and Peter R. Silverman in Toledo; Jaime Austrich; Erin Smith Aebel; Ernest J. Marquart; J. Todd Timmerman; and Rachel B. Goodman in Tampa; David H. Conaway, Jeffrey S. Bernard; Joseph J. Santaniello; and Steven A. Meckler in Charlotte; as well as David F. Axelrod in Columbus. The team includes the following attorney banking representatives to provide additional support to bank clients: Malcolm J. Pitchford (Sarasota); Martin D. Werner (Toledo); and W. Kent Ihrig (Tampa). The Shumaker Data Breach Team can assist in all aspects of data breach incidents including the prevention of data breaches as well as the ramifications after a breach.

For more information, contact Mike Taaffe at mtaaffe@slk-law.com or 941.364.2720.