Protect Yourself from the Next Cyber Attack

By Matthew D. Berkowitz and Joseph Greener

Recent cyber-attacks and data breaches affecting some of the world's largest companies present challenges directly applicable to background screeners and the private information they possess.

Only 37% of all businesses have a sophisticated method to track and control sensitive data.

Only 37% of all businesses have a sophisticated method to track and control sensitive data,[1] and 80% of companies take a week or more to realize they have even been the victim of a breach.[2]

In 2017, hackers breached Equifax's data system of social security numbers, dates of birth, email addresses, home addresses and driver's license numbers.[3] The data breach exposed 145.5 million people's personal information.[4]

The Equifax data breach has led to over 240 class-action lawsuits, over 60 investigations from state attorney generals and federal agencies, and an investigation from the Federal Trade Commission.[5] Most notably, a nationwide class action was filed in the United States District Court for the Northern District of Georgia with plaintiffs from every state and the District of Columbia.[6]

The number of cyber-attacks and data breaches are increasing. From 2014 to 2015, there was a 38% increase in cyber security incidents.[7] In 2013, Target reported that hackers stole credit and debit card information from up to 40 million shoppers during the holiday season.[8] Target ultimately paid $18.5 million to settle claims in 47 states and the District of Columbia.[9]

Home Depot paid $19.5 million to resolve a class-action lawsuit brought by victims of hackers who stole credit and debit card information from 56 million customers.[10] Additionally, two hackers stole the names, phone numbers and email addresses from 57 million Uber customers and driver's license numbers from 600,000 Uber drivers.[11] In the end, Uber paid $100,000 to the hackers to destroy the stolen data.[12]

These recent hacks and data breaches are a reminder that companies with sensitive information need to take proactive steps to protect themselves and the information that they possess. This is particularly true with respect to background check companies.

After a data breach, businesses can face lawsuits and significant exposure, ranging from statutory claims for violating various privacy statutes, negligence claims for failing to prevent the breach, negligence claims for failing to safeguard the sensitive information, claims for breach of contract, and claims for a breach of the covenant of good faith and fair dealing.

Continued on page 14

[1] *2014 State of Risk Response*, as quoted in Trustwave Security Stats.

[2] *2016 Data Breach Investigators Report* from Verizon.

[3] https://www.nytimes.com/2017/10/02/business/equifax-breach.html

[4] https://www.nytimes.com/2017/10/02/business/equifax-breach.html

[5] https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach/?utm_term=.b2c5e43a5449

[6] https://www.classaction.org/media/allen-et-al-v-equifax-inc.pdf

[7] https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

[8] https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

[9] https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

[10] https://www.csoonline.com/article/3041994/security/home-depot-will-pay-up-to-195-million-for-massive-2014-data-breach.html

[11] https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

[12] https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Protect Yourself from the Next Cyber Attack *Continued from page 13*

Currently, there is no comprehensive federal law governing the obligations of businesses to prevent and respond to data breaches.

Currently, there is no comprehensive federal law governing the obligations of businesses to prevent and respond to data breaches. However, on December 1, 2017, Senators Bill Nelson, Richard Blumenthal, and Tammy Baldwin introduced the Data Security and Breach Notification Act, requiring companies to report data breaches within 30 days and imposing criminal penalties of up to five years for knowingly concealing a data breach.[13] Although the bill is still under consideration,[14] it could provide increased obligations for background check companies as well as an additional cause of action against those companies for data breach victims.

There are several things that background screeners can do to protect themselves in the event of a data breach. Background screeners should take steps to track and control sensitive data by working with IT departments to add more password protections. Many companies will want to hire professional security organizations to conduct annual security assessments, or hire professional hackers to determine the vulnerability of their data.

Background screeners should also keep all of their data on a local network and limits that network's connection outside of the company. All sensitive data stored on the network should be encrypted and protected by user access controls to ensure that only authorized parties have access to the data.

The network should be monitored and upgraded periodically to prevent and log unauthorized access. Background check companies also need to physically secure all data. Companies often overlook the importance, and simplicity, of making sure their data is behind a physically locked door.

Background check companies should work with their insurance brokers and insurance carriers to ensure they have cyber liability insurance. Cyber liability insurance plans vary and can protect against the direct costs incurred from a data breach, including attorneys' fees and the costs of a computer forensic vendor. Cyber liability insurance can also protect against claims brought by third parties whose information was compromised.

These are some of the many ways background check companies can protect themselves from becoming the latest industry to experience the ramifications of a data breach and the class-action lawsuits that accompany them. ▲

Matthew D. Berkowitz is a Member of Carr Maloney P.C. He is an experienced civil litigator with significant class action experience who regularly defends background check companies and businesses accused of FCRA violations and other consumer protection violations.

Joseph B. Greener is an Associate of Carr Maloney P.C. He is a litigation attorney who focuses his practice on civil litigation, employment and labor law, civil rights, and Directors and Officers' liability.

napbs®
National Association of
Professional Background Screeners

[13] http://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html

[14] https://www.congress.gov/bill/115th-congress/senate-bill/2179/text