Paradigm

INTERNATIONAL SOCIETY OF PRIMERUS LAW FIRMS

SPRING 2015

The Perfect Storm

Primerus Firms Do Big Things with Technology

+

Current Legal Topics:

North America

Europe, Middle East & Africa

Latin America & Caribbean

Asia Pacific

Small, Medium-Sized Businesses Not Immune From Cyber Attacks and Data Breaches

Target, Home Depot, Chase Bank and now Sony Pictures Entertainment. Not a week goes by when news headlines aren't filled with announcements that another American-based company is the victim of a data breach or cyber attack. While larger companies are grabbing the most attention, small and medium-sized businesses (SMBs) are also at risk of having their sensitive customer (and even employee) data breached. Though less publicized, these breaches have occurred throughout the country and can have substantial impacts on "mom and pop" companies with limited resources.

Depending on the motives, SMBs may make more attractive targets for cyber-thieves. Because SMBs typically have fewer resources to combat these threats, cyber-thieves see SMB customer data as "low-hanging fruit." Hackers and other data thieves know these smaller companies often possess valuable customer information and may not be appropriately protecting this data from theft or inappropriate disclosure.

A data breach can be far more devastating for an SMB than a larger company. Although SMBs typically hold less customer data, hackers and data thieves who target SMBs are most likely motivated solely to use the customer data in an inappropriate manner. In contrast, hackers or data thieves who attack large corporations may have different motivations that are not solely for financial gain. For instance, some of the international hackers who have breached large corporations' data were politically motivated. Some are merely chasing the thrill of breaching large corporations' IT security systems and the resulting publicity, possibly never using or selling the stolen data.

The motivation to use customer data is particularly important. In consumer lawsuits dealing with data breaches, one of the key issues is whether the consumer's data has been used in an inappropriate or criminal manner. Financially-motivated hackers and data thieves typically sell the customer information they acquire or use it themselves to create fraudulent accounts or access existing accounts. Whether customers actually suffer economic losses from the misuse of their stolen information during a data breach could be paramount in determining the level of a company's potential financial exposure in litigation following a data breach. *Remijas v. The Neiman Marcus Group, LLC, 2014 U.S. Dist. LEXIS 129574 (N.D. Ill. 2014).*

While data breaches for large companies may not always be financially motivated (and therefore may not result in the misuse of stolen customer data), if a cyber attack occurs against a SMB, it can be presumed that the hackers/criminals targeted the business in order to misuse the customer data for their

Jonathan W. Macklem

J. Paul Zimmerman

Richard E. Smith

Jonathan W. Macklem represents and advises clients on a broad range of matters. He is a member of the firm's cyber and data breach liability, business and commercial litigation, insurance, labor and employment, and technology and emerging growth companies practice groups.

J. Paul Zimmerman's practice primarily focuses on business and commercial litigation in the areas of cyber and data breach liability, technology and emerging growth companies, trade secrets, insurance, and class action and complex litigation. He is a member of The Sedona Conference Working Group 1 and co-chair of CLM's eDiscovery and ESI Committee.

Richard E. Smith is one of Christian & Small's founding partners and has been an integral member of the firm's litigation group his entire legal career. His practice focuses primarily on complex and corporate litigation for clients in the financial services, health care and construction industries, as well as corporate entities in other industries.

Christian & Small LLP
505 North 20th Street
Suite 1800 Financial Center
Birmingham, Alabama 35203

205.545.7456 Phone
205.328.7234 Fax

jwmacklem@csattorneys.com
jpz@csattorneys.com
resmith@csattorneys.com
csattorneys.com

own financial gain. This means an increased risk for SMBs in terms of the damages to their clients/customers affected by the data breach. Under many applicable statutes and regulations, companies face exposure simply for the breach, even absent evidence of identity theft.

In addition to the potential for consumer lawsuits, other costs can be devastating for an SMB resulting from a data breach:

- **Determining the scope of the breach** – Companies will incur expenses in their efforts to identify and determine the scope of the data breach. This may involve costs to hire a computer forensic company and legal fees associated with this process.

- **Reputational harm** – SMBs can lose business if the community thinks the company has not taken appropriate measures to protect client information.

- **Business interruption** – It isn't uncommon for SMBs to have to shut down immediately following a data breach until the attack can be remediated. While a company's operational system is down, it could lose valuable revenue.

- **Notification requirements** – Myriad federal rules and regulations require companies in certain industries to provide notifications to customers affected by a data breach, and approximately 47 states have passed some form of a data breach notification law.

- **Regulatory proceedings** – Federal and even many state agencies are becoming increasingly active in investigating SMBs following data breaches. Many of these agencies are self-funded – their budgets consist of funds obtained through fines they impose. A government agency (or agencies) with jurisdiction over the SMB or the type of data involved may investigate whether a failure to meet a regulatory or statutory requirement was a factor in the data breach or theft. Additionally, credit card companies whose cards the SMB accepts as payment impose stringent data security and notification requirements – the violation of which can lead to fines, increased fees and even the termination of the ability to accept credit card payments.

There is also the threat that a data breach could occur from within the company, whether as retribution for perceived wrongs, financial gain, or both. It is important for SMBs to not only evaluate the security of their customers' information, but also evaluate who has access to that information within the company itself. Just as a company restricts its employees' access to checks and financial information, companies must also evaluate the appropriate limits for employee access to information such as customer or employee personal information and account information.

SMBs must particularly guard against two primary mechanisms for data breaches. First, hackers often target point-of-sale systems to access customers' financial information. It is imperative for companies that receive customer financial information to ensure their point-of-sale systems' security measures are compliant with the credit card industry's requirements.

Second, companies often find themselves in data breach situations because of a lack of precautions regarding technology (e.g., personal laptops/computers, employee cell phones, etc.). Human behavior and errors still account for about one-third of data breaches. Companies must evaluate the different devices where customer information is stored. Customer and employee information on portable devices should be encrypted, and a company should restrict employees' ability to store customer information on their own individual devices, such as personal computers, cell phones and tablets. The company should also have the ability to remotely wipe portable devices.

In light of the emerging data breach risks and their resulting costs, SMBs should work with their insurance agents or brokers to obtain appropriate insurance products to protect the company from a cyber attack or data breach. Over the last couple of years, the number of insurance companies writing cyber-liability policies has grown drastically. The protections and pricing for these policies can vary greatly, but policies can cover the costs associated with hiring a security firm to fix and contain the breach, in sending notification to affected customers, and providing defense and indemnity in the event lawsuits or regulatory investigations result from the breach. Some policies also provide coverage for public relations costs and business interruption coverage. Companies should not make the mistake of assuming their commercial general liability policy (CGL) will provide coverage for damages resulting from a data breach. SMBs should proactively work to protect against coverage gaps, ensuring appropriate insurance is in place.

SMBs must also evaluate their vendor contracts. Credit card companies and other financial institutions are now allocating the risk of loss upon vendors and companies whose lax data security led to a data breach. Lawsuits have been filed by credit card companies and banks seeking reimbursement of costs resulting from a company's alleged failure to act appropriately in the protection of customer information.

The costs of a data breach can be devastating for SMBs, so it is important for them to evaluate and utilize their data security practices and processes. A number of different companies provide security audits, although their qualifications vary greatly. These companies can develop strategies and evaluate security procedures on how best to minimize their data breach risk.

Overall, identity theft is the fastest-growing crime in the U.S. and, despite technological advancements, data breaches and cyber attacks are showing no signs of weakening in their frequency and sheer magnitude. SMBs should learn from recent headlines about major national and international companies by evaluating their own internal practices and procedures to minimize these risks. P