Client Alert – Happy Halloween!

6 *SCARY* Privacy and Data Security Facts and Recent Developments

October 31, 2016

This Halloween, it is not the ghost or goblin that should frighten your business – but rather, it is the ever expanding specter of liability that haunts businesses which fail to comply with privacy and data security laws. In honor of Halloween, Morse's privacy and data security team shares the following list of 6 ***SCARY*** recent developments and facts about privacy and data security.

1. ***Privacy Harms May Occur Absent Tangible Injury.*** In the Matter of LabMD, Inc., the Federal Trade Commission (FTC) clarified the scope of privacy harms that constitute "unfair" acts or practices under Section 5 of the Federal Trade Commission Act (the FTC Act). The FTC found that the data security practices of LabMD (a clinical laboratory that conducted tests on patient samples) were unreasonable, lacking even basic precautions. Among the unreasonable practices were LabMD's failure to use an intrusion detection system, to delete any of the consumer data collected, and to conduct any employee training. As a result of these failures, an employee had installed peer-to-peer file-sharing software on a LabMD computer (in order to listen to music at work) which caused a file containing the sensitive information of approximately 9,300 patients to be exposed on the peer-to-peer network. The FTC held that the mere fact that such sensitive information was exposed – without evidence of tangible injury, such as economic or physical harm to consumers – is in and of itself a substantial injury (and also likely to cause substantial injury) and therefore sufficient to support liability for unfair practices under the FTC Act.

2. ***Corporate Officers May Face Individual Liability.*** The Massachusetts data protection regulations (201 C.M.R. 17.00 et seq.) (the Regulations) apply to people and entities that collect or otherwise have access to "personal information" (as defined in the Regulations) of Massachusetts residents. The scope of the Regulations is broad and extends to out-of-state businesses. In addition, corporate officers may be exposed to ***individual liability*** for non-compliance. Specifically, the Regulations implement the provisions of Massachusetts General Laws Chapter 93H; violations of 93H are considered unfair practices under Chapter 93A, which imposes personal liability on corporate officers who are personally involved in unfair or deceptive business conduct. *See Nader v. Citron*, 372 Mass. 96, 103 (1977), *abrogated on other grounds; Community Builders, Inc. Indian Motocycle Assocs., Inc.*, 44 Mass. App. Ct. 537, 560 (1998). Corporate officers may also be exposed to individual liability under the federal analog to Chapter 93A (the FTC Act), *see F.T.C. v. Direct Mktg. Concepts, Inc.*, 624 F.3d 1, 12-13 (2010), which is regularly used to combat privacy and data security harms.

3. ***Failing To Proactively Address The Growing Threat Posed By Ransomware May Lead To Liability.*** According to recent U.S. Government Interagency Technical Guidance, more than 4,000 ransomware attacks have occurred daily since January 1, 2016, a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. Recognizing that companies of all types and sizes have been targets of ransomware, FTC Chairwoman Edith Ramirez recently noted that a company's failure to patch vulnerabilities known to be exploited by ransomware may violate the FTC Act.

4. ***The Common Practice Of Sharing Information With Third-Party Service Providers Is A***

Source Of Liability. Companies regularly share information with third-party service providers. However, there is liability associated with providing this access – both because substantial numbers of data breaches have been linked to third-party access and because companies fail to recognize their obligation to oversee these third parties under privacy and data security laws. Indeed, the Massachusetts Regulations (described above) impose such obligations. Ultimately, companies face increased risk if they do not: vet their third-party service providers' privacy and data security practices; impose contractual obligations to protect the information they share; and oversee service providers on an ongoing basis to verify compliance with these laws and contractual obligations.

5. ***Start-Ups Are Not Immune From Regulatory Scrutiny and Liability – Even Without A Breach***. Pursuant to its authority under the Dodd-Frank Wall Street Reform and Consumer Protection Act to take action against unfair, deceptive, or abusive acts or practices, the Consumer Financial Protection Bureau (CFPB), in its first privacy and data security action, entered into a Consent Order with Dwolla, Inc. a young financial technology company that operates an online payment platform. The CFPB found that Dwolla, on its website and in communications with consumers, misrepresented its data security practices by falsely claiming both that its data security practices "exceed" or "surpass" industry security standards and that information is "securely encrypted and stored". Although Dwolla had not suffered a data breach, the CFPB proactively investigated and prosecuted Dwolla, imposing a $100,000 penalty and requiring Dwolla to fix its security flaws and train employees.
6. ***There Are Significant Penalties for Violation of Privacy and Data Security Laws***. The penalties associated with violating privacy and data security laws can be significant, ranging from destruction of unlawfully obtained data to the payment of substantial monetary fines. Just this June, the FTC imposed $4 million in penalties (suspended to $950,000 based on the company's financial condition) on the mobile advertising network InMobi due to alleged misrepresentations concerning privacy practices and violation of the Children's Online Privacy Protection Act (COPPA).

Rather than being paralyzed with fear, companies should take proactive steps to comply with applicable privacy and data security laws, thereby mitigating risk and building trust. If you have questions about these matters, ***"Who you gonna' call?"*** Our privacy and data security team – Faith Kasparian (CIPP-U.S.), Mike Cavaretta, and Howard Zaharoff – of course!