

## Massachusetts Attorney General Enforcement Action: Data Breach, the Massachusetts Privacy Regulation and the Payment Card Industry Data Security Standard (PCI DSS)

*Melissa J. Krasnow, Dorsey & Whitney LLP*

In March 2011, a Final Judgment by Consent was issued in *Massachusetts v. Briar Group, LLC*, which involves a 2009 Massachusetts data breach and implicates the Massachusetts privacy regulation and the Payment Card Industry Data Security Standard ("PCI DSS").<sup>1</sup>

The Massachusetts privacy regulation applies to a person or entity that owns or licenses personal information about a Massachusetts resident, meaning their first and last name or first initial and last name in combination with a (i) Social Security Number, (ii) driver's license or state-issued identification card number or (iii) financial account number or credit card or debit card number. Such person or entity must implement and maintain a comprehensive, written information security program. The Massachusetts Attorney General enforces the Massachusetts privacy regulation. The deadline for compliance with the Massachusetts privacy regulation was March 1, 2010.<sup>2</sup>

The Payment Card Industry Security Standards Council (including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.) sets and enforces PCI DSS, which contains requirements for a secure payments environment framework for any business that stores, processes or transmits payment cardholder

data. For example, a business that accepts or processes payment cards must comply with PCI DSS. Interestingly, the following three states have laws addressing compliance with PCI DSS – Minnesota (which is based on, but does not specifically reference, PCI DSS) and Nevada and Washington (which each specifically reference PCI DSS).<sup>3</sup>

The Briar Group, a Boston restaurant chain owner and operator, reported a data breach to the Massachusetts Attorney General on or around November 24, 2009. In April 2009, the Briar Group experienced a data breach when malware was installed on its computer systems and allowed hackers access to customers' credit card and debit card information, including names and account numbers. The malware was not removed from the Briar Group's computers until December 2009.

The Briar Group entered into an agreement to resolve the alleged claims of the Massachusetts Attorney General that the Briar Group engaged in unfair or deceptive acts or practices in violation of the Massachusetts consumer protection law by accepting credit card and debit cards from consumers for transactions at their restaurants but failing to protect their personal information.<sup>4</sup> Hackers using malware were possibly able to gain access the computer system of the Briar Group and extract cus-

---

© 2011 Dorsey & Whitney LLP. Originally published by Bloomberg Finance L.P. in the Vol. 3, No. 16 edition of the Bloomberg Law Reports—Technology Law. Bloomberg Law Reports<sup>®</sup> is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

tomers credit card and debit card information due to the failure of the Briar Group to implement basic data security measures.

Specifically, this included (i) failing to comply with PCI DSS, (ii) failing to change default user names and passwords on its Micros Point of Sale computer system, (iii) failing to change passwords in its computer network for more than five years, (iv) allowing multiple employees to share common usernames and passwords, (v) failing to modify passwords after employee termination or resignation, (vi) failing to adequately control the number of employees with administrative access to the Briar Group's computer network, (vii) failing to properly secure remote access utilities and wireless network, (viii) continuing to accept consumer credit cards and debit cards when the Briar Group knew of a data breach and failing to alert its patrons to the data breach while malware remained on its computer system and (ix) storing payment card information in clear text on its servers.

The Briar Group agreed to (i) comply with and verify its compliance with PCI DSS with the Massachusetts Attorney General's Office, (ii) not knowingly maintain on its network after the authorization process the full contents of the magnetic stripe of a credit card or debit card, or of any single track of such stripe, or the CVC2/CVV2/CID of any such card or the PIN or PIN block of any such card, (iii) implement, maintain and adhere and produce to the Massachusetts Attorney General's Office a written information security program under 201 CMR § 17.00, (iv) review the scope of its security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information under 201 CMR § 17.03(i), (v) implement security password management for portions of its computer system that store, process or transmit personal information (including its Micros Point of Sale computer systems), (vi) implement security password management where each person with access to its computer networks is

assigned a unique ID and (vii) segment appropriately from the rest of its computer system the network-based portions that store, process or transmit personal information, by firewalls, access controls or other appropriate measures. The Briar Group also was required to pay \$110,000 in civil penalties to Massachusetts.

Finally, the Briar Group must contact a Qualified Incident Response Assessor to investigate a suspected data compromise if it receives notice from a credit card company, payment card processing company, bank or law enforcement agency requiring a forensic audit of its Point of Sale Systems and related infrastructure because a Common Point of Purchase or similar analysis linked fraudulent transactions to Briar Group establishments. If the Briar Group is unable to conclude whether a data compromise has occurred within 14 days of retaining a Qualified Incident Response Assessor, the Briar Group will (i) post conspicuous notice in each of its potentially affected establishments alerting customers that their debit cards and credit cards might be at risk due to a suspected data compromise and (ii) provide a copy of this consumer notice to the Massachusetts Attorney General's Office.

*Melissa J. Krasnow is a partner in the Corporate Group of Dorsey & Whitney LLP who also is a Certified Information Privacy Professional and serves on the International Association of Privacy Professionals Publication Advisory Board.*

---

<sup>1</sup> *Commonwealth of Massachusetts v. Briar Group, LLC*, Civ. No. 11-1185B, Consent Judgment (Mass. Sup. Ct. Mar. 28, 2011).

<sup>2</sup> 201 CMR § 17.00 et seq. (For additional information about the Massachusetts privacy regulation, please see Melissa J. Krasnow, *Final Massachusetts Privacy Regulation: What is Required and How to Comply*, Bloomberg Law Reports - Risk & Compliance, Vol. 2, No. 12 (Dec. 2009).

<sup>3</sup> Minn. Stat. § 325E.64; Nev. Rev. Stat. § 603A.215; Rev. Code Wash. § 19.255.020. (For additional information about the Nevada and Washington laws,

please see Melissa J. Krasnow, *Revised Nevada Privacy Law Furthers Encryption and Payment Card Law Trends*, Bloomberg Law Reports - Technology Law, Vol. 1, No. 3 (Aug. 24, 2009), and *Washington Continues the Trend of Encryption and Payment Card Laws*, Bloomberg Law Reports - Privacy Law, Vol. 3, No. 5 (June 2010).

4 Mass. Gen. Laws ch. 93A § 2.