

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION NO.

11-1185 ¹³

COMMONWEALTH OF MASSACHUSETTS,)
)
Plaintiff,)
)
v.)
)
BRIAR GROUP, LLC,)
)
Defendant.)

COMPLAINT

SUFFOLK SUPERIOR COURT
 CIVIL CLERK'S OFFICE
 2011 MAR 28 AM 8:41
 MICHAEL JOSEPH DONOVAN
 CLERK/MAGISTRATE

I. INTRODUCTION

1. The Commonwealth of Massachusetts, by and through its Attorney General, Martha Coakley, brings this action against Defendant Briar Group, LLC ("Briar"), pursuant to G. L. c. 93A, § 4.

2. Briar engaged in unfair and deceptive conduct, pursuant to G. L. c. 93A, in connection with a data breach, wherein malware was installed on Briar's computer system. Briar was alerted to this data breach on or around October 29, 2009. Due to Briar's failure to implement basic data security measures on its computer system, hackers were able to gain access to data processed on Briar's computer system and extract customers' credit and debit card information during the period of April 2009 through December 2009. From October 29, 2009, when Briar learned of the data breach, to December 10, 2009, when a computer forensics company removed the malware, Briar committed additional unfair and deceptive acts by failing to alert its patrons to the data

breach, and continuing to accept credit and debit cards from Briar customers without taking reasonable steps to safeguard customers' personal information.

3. By this action the Commonwealth seeks penalties, costs, attorney's fees, and restitution pursuant to G. L. c. 93A, the Massachusetts Consumer Protection Act. The Commonwealth also seeks injunctive relief as may be determined to be appropriate and equitable in order to remedy, address, and prevent future harm arising from Briar's unfair and deceptive conduct.

II. JURISDICTION AND VENUE

4. The Attorney General is authorized to bring this action pursuant to G. L. c. 93A, § 4 and G. L. c. 12, § 10.

5. This Court has jurisdiction over the subject matter of this action pursuant to G. L. c. 93A, § 4, G. L. c. 12, § 10, and G. L. c. 223A, § 3.

6. Venue is proper in Suffolk County pursuant to G. L. c. 223, § 5 and G. L. c. 93A, § 4.

III. THE PARTIES

7. The plaintiff is the Commonwealth of Massachusetts, represented by the Attorney General, who brings this action in the public interest pursuant to G. L. c. 12, § 10 and G. L. c. 93A, § 4.

8. The defendant, Briar, is a Massachusetts corporation with a principal place of business at 311 Washington Street, Brighton, Massachusetts. Austin M. O'Connor is the President of Briar.

IV. STATEMENT OF FACTS

A. BACKGROUND

9. Briar is a Massachusetts corporation which operates several restaurants and bars in the Boston area, including The Lenox, MJ O'Connor's, Ned Devine's, The Green Briar, and The Harp.

10. On November 25, 2009, the Attorney General's Office received a notification, dated November 24, 2009, alerting the Attorney General to a data breach at Briar, which impacted the credit and debit card information of tens of thousands of consumers who used their cards at the various Briar establishments. As a result of Briar's failure to reasonably and appropriately secure consumer credit and debit card information, including names and account numbers, over 53,000 MasterCard accounts and over 72,000 Visa accounts were affected by the data breach, providing a channel for the infliction of fraud on consumers and forcing consumers and their banks to endure the inconvenience, cost, and uncertainty of cancelling and re-issuing thousands of credit and debit cards used at Briar.

11. Briar engaged in unfair and deceptive conduct that led to the breach of thousands of consumers' payment card information because it failed to implement basic data security measures on its computer system to protect the personal information of its customers, despite the fact that it conducts approximately 238,000 Visa and MasterCard credit and debit card transactions on an annual basis, totaling over \$9 million per year, at the six Briar locations impacted by the data breach.

12. Defendant accepts credit and debit cards from its consumers on a daily basis in order to facilitate transactions at Briar's restaurants and bars, yet failed to take

the most basic steps to protect the personal information obtained from its patrons. Defendant's unfair and deceptive conduct includes its: (a) failure to change default usernames and passwords on its Micros Point of Sale computer system; (b) failure to change passwords in its computer network for more than five years; (c) failure to control the sharing of common usernames and passwords among multiple employees; (d) failure to modify passwords after termination or resignation of employees; (e) failure to adequately control the number of employees with administrative access to Briar's computer network; (f) failure to properly secure its remote access utilities and wireless network; (g) failure to alert Briar patrons to the data breach between the time it learned of the data breach and the time the malware was removed from its computer system and the fact that it continued to accept credit and debit cards from Briar consumers during this time period despite its knowledge of the data breach; (h) storage of payment card information in clear text on its servers; and (i) failure to comply with Payment Card Industry Data Security Standards.

B. THE DEFENDANT IS ALERTED TO FRAUDULENT ACTIVITY ON CREDIT AND DEBIT CARDS LAST LEGITIMATELY USED AT BRIAR ESTABLISHMENTS.

13. On October 15, 2009, a payment card processing company based in Europe noticed possible fraudulent activity relating to several credit and debit card accounts. The payment card processing company determined that the affected cards had last been legitimately used at several Common Points of Purchase ("CPPs") and realized that the CPPs were all located in Boston, Massachusetts.

14. Upon further analysis, the payment card processing company determined that the affected cards had been last legitimately used at restaurants and venues that were

all owned and operated by Briar. The initial breach occurred at Briar's 'Ned Devine's' location in Faneuil Hall in Boston, but the breach also affected the following Briar locations: The Lenox, The Harp, MJ O'Connor's Back Bay, MJ O'Connor's Waterfront, and The Green Briar.

15. The payment card processing company notified Visa and MasterCard of the fraudulent activity on October 20 and 21, 2009, respectively. Subsequently, Visa and MasterCard also learned from other card issuers that payment card accounts used legitimately at Briar restaurants and bars were later used for fraudulent transactions.

16. On October 20, 2009, Visa contacted Sovereign Bank, the acquirer for Briar's payment card transactions. An acquirer is the financial institution that enters into agreements with merchants, such as Briar, to accept cards as payment for goods and services.

17. Sovereign Bank then contacted First Data about the data breach. First Data provides merchant processing and card acquirer services for Sovereign Bank and manages payment card transactions with Sovereign Bank's merchants. Briar received notice of the security breach from First Data on or around October 29, 2009.

18. On November 13, 2009, Citigroup Security Services also notified Briar that cardholder accounts used for fraudulent transactions were linked to six establishments belonging to Briar by Common Point of Purchase analysis.

C. THE DEFENDANT COMMITTED UNFAIR OR DECEPTIVE ACTS OR PRACTICES BY FAILING TO TAKE BASIC PRECAUTIONS TO PROPERLY SECURE ITS COMPUTER NETWORK AND CONTINUING TO ACCEPT CREDIT AND DEBIT CARDS FROM CONSUMERS AFTER LEARNING OF THE DATA BREACH, WHILE MALCODE REMAINED ON ITS SERVERS.

19. The president of Briar, initially expressed reluctance to hire a computer forensics company to investigate the data breach affecting Briar's bars and restaurants. In a November 5, 2009 e-mail, Briar's president noted that he wanted "to do the right thing" but did not want to have to "pay for an investigation that they could somehow avoid."

20. Three weeks after Briar was notified by First Data of the breach, and after being required by Visa to retain a Qualified Incident Response Assessor, Briar engaged Verizon Business Network Services ("VBNS") to conduct a forensic investigation of its computer network and Point of Sale terminals. VBNS arrived at Briar's headquarters on or around November 15, 2009, to begin its investigation. While on-site, VBNS acquired forensic images of Briar's servers and workstations in order to analyze the scope and extent of, and the reasons behind, the data breach.

21. VBNS provided frequent updates to Briar while it conducted its investigation, including an initial draft of its report on December 13, 2009. After exchanging multiple drafts of its report and incorporating Briar's comments into its report, VBNS provided Briar with a final computer forensics report on or around January 4, 2010. VBNS found that a data breach had in fact occurred because a network system had been breached, allowing an intruder to access magnetic stripe cardholder information in the form of full Track 1 and Track 2 Data, after installing malcode on Briar's server on April 24, 2009. There are two tracks of data on a bankcard's magnetic

stripe: Track 1 data contains the account number, the cardholder name, and the additional data listed on Track 2. Track 2 contains the account number, expiration date, and secure code.

22. As described in VBNS' report on Briar's data breach, malcode or malware "is considered an application or script illegitimately used to damage system files and/or operation by recording user keystroke data, slowing down or spamming systems, deleting files, and other often covert and illegitimate activities." The installation of malcode was evidenced by creation of the folder "C:\\WINDOWS\\system32\\memdump" on each of Briar's six compromised Micros 9700 Point of Sale servers. In a typical Briar transaction a customer's credit or debit card is swiped at a Micros 9700 Point of Sale terminal, and the information is passed to the Micros 9700 Point of Sale server. The malcode installed on Briar servers was a memory dumping program, designed to dump information, including payment card data, that was contained on the Point of Sale servers. The malcode program parsed through the memory dumps for payment card data and saved it in an output file, "inetinfo.ch," that contained the Tracks 1 and 2 data.

23. The malcode was not removed from Briar's systems until December 10, 2009.

24. From October 29, 2009, when Briar learned of the data breach, to December 10, 2009, when VBNS removed the malcode, Briar continued to accept credit and debit cards from its customers and failed to alert its patrons to the data breach.

25. The intruder was able to access Briar's home server and from there was able to access the other restaurant locations and install malcode because all of the affected locations were constructed on a flat network on a single Windows Domain. A

flat network is a network in which workstations are directly connected to one another, without intermediary hardware devices. The Micros 9700 Point of Sale servers had remote access utilities, including pcAnywhere and Microsoft Remote Desktop, enabled at the system start. The open configuration of these utilities allowed access of the Micros 9700 servers from the Internet.

26. Essentially, according to VBNS, the malware installed on Briar's systems likely operated as follows: when customers' credit or debit cards were swiped at the point of sale, payment card data could be captured and then exported to a file, from which the data could be exfiltrated to unauthorized persons.

27. VBNS found that the network was susceptible to this type of attack because of Briar's open remote access applications over the Internet and because Briar had failed to change the default username and passwords on its Micros Point of Sale system. These default credentials are designed to be modified to reflect user specific names and passwords after installation of the server. The intruder who installed the malware on the systems did so with the default user credentials, which Briar failed to change, and which were used system wide for all users, rather than assigned user specific names and passwords.

28. Briar knew or should have known that failing to change the default username and password on its Micros Point of Sale system could easily allow a data breach of its computer network. As noted by VBNS, Briar's "default setting is the most significant factor contributed to the attack, as the default credentials are known throughout the hacker community."

29. Wireless networks were available at each of the affected locations, but did not have any security enabled on them, such as Wi-Fi Protected Access. The wireless and wired networks connected to a firewall, but were not properly segmented as the Micros Point of Sale system was reachable once a user connected to Briar's wireless network. Briar should have but failed to restrict the connections to its networks and systems that contained cardholder data.

30. In addition, as stated by VBNS in its report, "a password management policy does not exist within The Briar Group. It was determined through interviews with Bromley Engineering personnel that most passwords have not been changed in over five years, and default passwords were used on the Micros systems. Passwords were also shared among users and were not modified after termination or resignation of employees." Briar outsourced its technical infrastructure and support to Bromley Engineering.

31. Furthermore, Briar Group granted all of its employees local Administrator access on their assigned desktop computers, thus imposing no limitation on the software that could be installed on corporate equipment.

32. VBNS, in its forensic investigation, also discovered 7,130 instances where unencrypted cardholder account number and expiration dates, in clear text, were retained on the Micros 9700 Point of Sale server at Ned Devine's. Although VBNS did not find evidence that this particular information was exfiltrated by hackers, it did recommend that Briar regularly audit its systems to ensure that cardholder data is not improperly stored.

D. BRIAR FAILED TO COMPLY WITH PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS UNTIL APRIL 2010.

33. At the time of the data breach, Briar, despite being required to do so by Visa and MasterCard, did not adhere to Payment Card Industry Data Security Standards (“PCI DSS”).

34. PCS DSS is a standard of security set by several major credit card companies, including Visa and MasterCard, to protect cardholder data. Although, at VBNS’ recommendation Briar did change its password management policy and improve its system security, Briar failed to validate its PCI compliance until April 21, 2010, almost six months after it learned of the data breach, nearly a year after malware was installed, and only after it was fined by Visa and MasterCard for continued non-compliance with PCI DSS following the data breach.

35. At the time of the data breach Briar failed to meet the following PCI DSS requirements because it:

- a) failed to install and maintain a firewall configuration to protect data;
- b) used vendor-supplied defaults for system passwords and other security parameters;
- c) failed to protect stored data;
- d) failed to develop and maintain secure systems and applications;
- and
- e) failed to assign a unique ID to each person with computer access.

36. As noted by VBNS, it “is not aware of any reports of an organization that was fully compliant with PCI becoming the victim of account data compromise.”

37. Briar knew or should have known that failing to maintain PCI DSS compliance greatly increased the risk that it would be subject to a data breach.

38. Briar knew or should have known of the problems with the security of its network prior to the data breach, but failed to take even minimal action to protect the personal information of its customers. Peter Bromley, of Bromley Engineering, noted in a December 2, 2009, e-mail to Briar that Briar's security "problems came up years ago when I first returned to Briar and saw the blatant lack of [] even basic security on the Micros servers." Mr. Bromley also noted in a March 25, 2010 e-mail to Briar that: "Probably the most egregious practice had been that all Micros servers with which I have had contact used the same administrator name and password – even at different restaurants."

39. Briar, which conducts hundreds of thousands of credit and debit card transactions every year, should have implemented basic security on its computer systems, including changing default passwords. Briar should not have continued to accept credit and debit cards from its consumers after it learned of the data breach, while malware remained on its servers, and it knew or should have known that its failure to implement basic data security measures to protect the payment card information of tens of thousands of its customers was unfair and deceptive in violation of G. L. c. 93A, § 2(a).

40. Briar's failure to implement basic security on its computer system led to the exfiltration of the credit and debit card information of tens of thousands of its customers. Due to Briar's failure to protect customers' information, fraudulent purchases using information stolen from Briar occurred in multiple national and international

locations including Arizona, California, Nevada, Texas, the United Kingdom, Italy, India, and Saudi Arabia.

41. On November 22, 2010, the Attorney General sent Briar a letter, pursuant to G. L. c. 93A, § 4, notifying it of this intended action, and giving Briar the opportunity to confer with the Attorney General.

V. CAUSES OF ACTION

COUNT I (Violations of G. L. c. 93A)

42. The allegations contained in paragraphs 1-41 of the Complaint are realleged and incorporated herein by reference.

43. Defendant engaged in unfair or deceptive acts or practices, in violation of G. L. c. 93A, § 2, by accepting credit and debit cards from its consumers in order to facilitate transactions at Briar's restaurants and bars, yet failing to take reasonable steps to protect the personal information obtained from its patrons. Defendant's failure to implement basic data security measures to protect consumers' credit and debit card information includes, but is not limited to the following:

- a. failing to change default usernames and passwords on its Micros Point of Sale computer system;
- b. failing to change passwords in its computer network for more than five years;
- c. allowing multiple employees to share common usernames and passwords;
- d. failing to modify passwords after termination or resignation of employees;

- e. failing to adequately control the number of employees with administrative access to Briar's computer network;
- f. failing to properly secure its remote access utilities and wireless network;
- g. continuing to accept credit and debit cards from consumers when Briar knew of the data breach and failing to alert its patrons to the data breach while malware remained on its computer system;
- h. storing payment card information in clear text on its servers; and
- i. failing to comply with Payment Card Industry Data Security Standards.

44. Each of these acts or failures to act set the stage for a data breach by which hackers obtained tens of thousands of credit and debit card numbers, and used that information for fraudulent purposes. More than 125,000 consumers were harmed by Briar's conduct.

PRAYERS FOR RELIEF

WHEREFORE, the Commonwealth requests that the Court grant the following relief:

1. Order that the Defendant refrain from violating G. L. c. 93A;
2. Order that the Defendant implement, maintain, and adhere to a Written Information Security Program ("WISP") pursuant to 201 CMR 17.00 and produce said WISP to the Attorney General's Office;
3. Order that, pursuant to 201 CMR 17.03(i), Defendant review the scope of its security measures at least annually or whenever there is a material

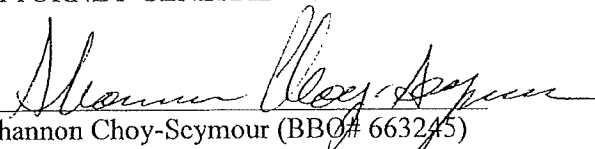
change in business practices that may reasonably implicate the security or integrity of records containing personal information;

4. Order that the Defendant maintain its PCI DSS compliance, and verify with the Attorney General's Office its compliance with PCI DSS;
5. Order that the Defendant make restitution, plus interest, to any consumer who was injured by any acts and practices found to have violated G. L. c. 93A, § 2(a), including those known and not yet known to the Attorney General;
6. Order that the Defendant pay civil penalties and costs of investigation and litigation of this matter, including reasonable attorney's fees, to the Commonwealth pursuant to G. L. c. 93A, § 4.
7. Order such other and further relief as this Court deems just and proper.

Respectfully Submitted,

COMMONWEALTH OF
MASSACHUSETTS

MARTHA COAKLEY
ATTORNEY GENERAL

By: 
Shannon Choy-Scymour (BBO# 663245)
Assistant Attorney General
Consumer Protection Division
One Ashburton Place
Boston, MA 02109
(617) 727-2200
shannon.choy-seymour@state.ma.us

Date: March 28, 2011