IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JEREMY WILLIAMS, on behalf of himself and a class,	)
Plaintiff,	)
v.	)
MICHAELS STORES, INC., a Delaware corporation,	)
Defendant.	)

COMPLAINT – CLASS ACTION

MATTERS COMMON TO MULTIPLE CLAIMS

INTRODUCTION

1. This complaint seeks redress for the conduct of defendant Michaels Stores, Inc. (“Defendant” or “Michaels”) for failing to secure and safeguard its customers' personal financial data, including credit and debit card information and PIN numbers.

2. Count I seeks relief under the Federal Stored Communications Act, 18 U.S.C. § 2702 et seq. Count II alleges violation of the Illinois Consumer Fraud Act. Count III alleges breach of contract.

NATURE OF THE ACTION

3. On information and belief, Michaels knowingly violated federal and state law by failing to take commercially reasonable steps to protect plaintiff and class members' personal financial information. Michaels' lack of adequate security granted easy access to third-parties who tampered with in-store PIN pads to "skim" unwitting customers' debit and credit card information and subsequently steal money directly from the victims' bank accounts. Michaels' security failure enabled thieves to steal customer financial data from within the retailer's stores and subsequently loot the customers' bank accounts from remote automated teller machines ("ATMs").

4. Michaels uses PIN pads to process its customers' in-store debit and credit card payments. A PIN pad is an electronic device used in a debit or credit card-based transaction to input and encrypt the cardholder's personal identification number, or PIN. PIN pads are normally used with integrated point of sale devices in which an electronic cash register is responsible for taking the sale amount and initiating/handling the transaction. The PIN pad is required so that the customer card can be accessed and the PIN can be securely entered, stored and encrypted before it is sent to the transaction manager or the bank for verification.

5. On information and belief, Michaels failed to employ commercially reasonable security measures. Michaels' failure to secure its customers' debit and credit card information led to a security breach that exposed the financial data and bank account balances of customers who shopped at 90 Michaels stores across 20 states between February 8, 2011 and May 6, 2011. The stores are listed in Exhibit A, attached.

6. On May 5, 2011, almost three months after the skimming scheme began, Michaels sent a belated Customer Security Alert to some of its customers via email (the "email Alert"). The email Alert was signed by Michaels' Chief Executive Officer, John B. Menzer. It began, "Michaels has just learned that it may have been a victim of PIN pad tampering in the Chicago area and that customer credit and debit card information may have been compromised." The email Alert then urged customers to "protect themselves" by "immediately contacting [their] bank and/or credit card company to check for and report any unauthorized charges, as well as seek their advice on how to protect [their] account in the event that [their] information has been taken."

7. Michaels failed to send the email Alert to all of its customers, including Plaintiff, and it did not otherwise pursue commercially reasonable measures to notify its customers about the security breach. In any event, Michaels' email Alert failed to provide timely and clear notification to anyone, thereby preventing customers from taking meaningful, proactive steps to secure their financial data and bank accounts.

8. In failing to provide adequate data security and timely notice of the security breach, Michaels violated federal and Illinois consumer protection statues.

PARTIES

9. Plaintiff Jeremy Williams is a citizen of Illinois who resides in the Northern District of Illinois.

10. Defendant, Michaels Stores, Inc. is a Delaware corporation with its principal place of business in Irving, Texas. Defendant is North America's largest specialty arts and crafts retailer with more than 964 stores located in the United States.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5 million, exclusive of interest and costs, and plaintiff, as well as most members of the proposed class, are citizens of states different from the state of the defendant. This Court also has subject matter in jurisdiction pursuant to 28 U.S.C. §1331.

12. This Court has personal jurisdiction over Michaels because Michaels does business in Illinois and has stores in Illinois.

13. Venue is proper in this Court under 28 U.S.C. § 1391(a) because a substantial part of the events giving rise to the claims enumerated herein occurred in this judicial district.

FACTS RELATING TO PLAINTIFF

14. At the end of March 2011, plaintiff used his TCF Bank debit card to purchase merchandise from the Michaels store in Burbank, Illinois.

15. Plaintiff swiped his debit card through one of the tampered Michaels PIN pads and unwittingly had his debit card information and PIN number stolen as a result.

16. On May 4, 2011, TCF Bank called plaintiff, leaving a recorded message advising him of ATM transactions made on his account.

17. Plaintiff returned the call and was made aware of 2 transactions in California that he had not engaged in or authorized.

18. After plaintiff was informed of the unauthorized ATM transactions in California, he deactivated his debit card.

19. The two unauthorized withdrawals from his checking account occurred on May 4, 2011 at an ATM located at 21901 Sherman Way, Los Angeles, California in the amount of $303.00 and $203.00.

20. Plaintiff talked to his bank on May 4, 2011 and reported the theft to his local police.

21. On information and belief, the debit card information had been "skimmed" from Michaels.

22. Like numerous other consumers who filed complaints, plaintiff never received any alert or notification about the security breach from Michaels.

23. Plaintiff was charged $175 in NSF fees by his bank as a result of the unauthorized transactions.

FACTS RELATING TO MICHAELS' REPRESENTATIONS TO THE CLASS

24. Michaels represented to its customers in its privacy policy (Exhibit B):

a. "In general, we do not share personal information outside of Michaels unless we have clearly asked for and obtained explicit consent."

b. "We are committed to keeping personal information secure. We have appropriate technical, administrative, and physical procedures in place to protect personal information from loss, misuse or alteration.

c. "We limit access to personal information to those who have a

business need. We keep personal information only for a reasonably needed amount of time."

d. "When we collect or transmit sensitive information such as credit card numbers, we use industry standard methods to protect that information."

FACTS RELATING TO "SKIMMING"

25. Skimming is the unauthorized capture of debit and/or credit card magnetic strip data. Magnetic strip technology can be duplicated easily, making it quick and simple for crooks to assume a victim's identity.

26. Skimming can occur during routine ATM or payment transactions. One of the most common methods for thieves to steal PIN pad information is by using a "skimmer." These devices are typically constructed with easily obtainable electronic parts.

27. First, thieves use false card readers combined with hidden wireless cameras or electronic membranes placed over the PIN keypads to capture a victim's card information and PIN numbers. Second, the captured information is then transmitted to the thieves, who may sell the information online or use it to create a bogus duplicate card. Creating duplicate cards takes only seconds using a card cloning machine that can be purchased online. Finally, low-level crooks called "cashers" use the bogus card–complete with stolen PIN-to withdraw cash directly from the victim's bank accounts via ATMs.

28. According to the Electronic Funds Transfer Association, theft from ATM skimming exceeds $1 billion annually.

29. On information and belief, Michaels failed to take commercially reasonable steps to safeguard customer financial information. Michaels did not employ appropriate technical, administrative, or physical procedures to protect customer financial information from unauthorized capture, dissemination, or misuse, thereby making its consumers

an easy target for third-party skimmers.

30. Michaels has admitted that PIN pads at its stores in 20 states were fitted with skimming devices.

31. Tamper-proof payment terminals have been commercially available for a number of years. Use of such terminals makes skimming difficult or impossible. On information and belief, the PIN pads that were fitted with skimming devices were not tamper-proof terminals.

32. The security breach affected checkout line terminals at stores in Illinois, Colorado, Delaware, Georgia, Iowa, Massachusetts, Maryland, North Carolina, New Hampshire, New Jersey, New Mexico, Nevada, New York, Ohio, Oregon, Pennsylvania, Rhode Island, Utah, Virginia and Washington.

33. Upon information and belief, during the weekend of April 30 - May 1, 2011, class members complained to local law enforcement authorities in the greater Chicago area about unauthorized withdrawals from their bank accounts in connection with use of a debit card while shopping at Michaels stores.

34. Michaels first notified some of its customers about the security breach on May 5, 2011 through the email Alert. Upon information and belief, Michaels knew of the security breach prior to May 5, 2011. However, Michaels failed to take immediate action to prevent the further dissemination of consumer financial information and theft of consumer bank account funds.

35. In response to the theft, Michaels customer service representatives are merely urging class members to "watch [their] account" and "inform [their] bank or card company and the authorities of any unauthorized activity." Thus, Michaels is placing the burden on aggrieved customers, like Plaintiff, either to self-monitor their accounts and credit reports for years to come, or to purchase professional credit monitoring services in the wake of the security breach and theft. At no time has Michaels offered any credit monitoring assistance to plaintiff.

CLASS ACTION ALLEGATIONS

36. Pursuant to Fed. R. Civ.P. 23(a) and (b)(3), plaintiff seeks to represent a class defined as all persons who made an in-store purchase at a Michaels store affected by payment card tagging using a debit or credit card that was swiped through a PIN pad at any time from February 8, 2011 through present (the "Class"). Exhibit A lists stores affected by payment card tagging; other stores may later be determined to have been affected by payment card tagging.

37. Plaintiff seeks to represent a subclass consisting of class members whose transactions occurred in Illinois.

38. Members of the class are so numerous that their individual joinder herein is impracticable. On information and belief, there are thousands of Michaels customers who suffered a loss of money and breach of security. Class members may be notified of the pendency of this action by mail, email and/or publication.

39. Common questions of law and fact exist as to all class members and predominate over questions affecting only individual class members. These common legal and factual questions include, but are not limited to:

a. Whether Michaels failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive financial information.

b. Whether Michaels properly implemented its purported security measures to protect customer financial information from unauthorized capture, dissemination, and misuse.

c. Whether Michaels took reasonable measures to determine the extent of the security breach after it first learned of the same.

d. Whether Michaels' delay in informing consumers of the security breach was unreasonable.

e. Whether Michaels' method of informing consumers of the security breach and its description of the breach and potential exposure to damages as a result of the same was unreasonable.

f. Whether Michaels' conduct violates the Stored Communications Act, 18 U.S.C.§ 2702.

g. Whether Michaels' conduct involved unfair and/or deceptive acts and practices, in violation of 815 ILCS 505/2.

h. Whether Michaels' conduct violated its contracts with plaintiff and class.

40. Plaintiff's claims are typical of the claims of the class members. Each class member was subjected to the same illegal conduct, was harmed in the same way, and has claims for relief under the same legal theories.

41. Plaintiff is an adequate representative of the class because plaintiff's interests do not conflict with the interests of the class members plaintiff seeks to represent, plaintiff has retained counsel competent and experienced in prosecuting class actions, and plaintiff intends to prosecute this action vigorously. The interests of class members will be fairly and adequately protected by plaintiff and counsel.

42. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of class members. Each individual class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Michaels' liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of

Michaels' liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I – FEDERAL STORED COMMUNICATIONS ACT,18 U.S.C. §2702

43. Plaintiff incorporates paragraphs 1-42.

44. This claim is brought on behalf of the class.

45. The Stored Communications Act ("SCA") contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S.Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3557.

46. Section 2702(a)(1) of the SCA provides "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. §2702(a)(1).

47. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* at § 2510(15).

48. Through its payment processing equipment (including its PIN pads), Michaels provides an "electronic communication service to the public" within the meaning of the SCA because it provides consumers at large with credit and debit card payment processing capability that enables consumers to send or receive wire or electronic communications concerning their account data and PINs to transaction managers, card companies or banks.

49. On information and belief, by failing to take commercially reasonable steps to safeguard sensitive consumer financial data, Michaels has knowingly divulged customer credit and debit card account information and PINs that were communicated to financial institutions solely for the customer's payment verification purposes while in electronic storage in

Michaels' PIN pads.

50. Section 2702(a)(2)(A) of the SCA provides "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A)

51. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

52. An "electronic communications system" is defined by the SCA as "any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

53. Michaels provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photo optical, or photoelectric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer financial information, and the use of PIN pads for the electronic storage of such communications during the payment verification process.

54. By failing to take commercially reasonable steps to safeguard sensitive consumer financial data, Michaels has knowingly divulged customer credit and debit card account information and PINs that were carried and maintained on Michaels' remote computing service solely for the customer's payment verification purposes.

55. As a result of Michaels' conduct described herein and its violations of

§2702(a)(1) and (2)(A), plaintiff and class members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft.

WHEREFORE, the Court should enter judgment in favor of Plaintiff and the Class and against Michaels for:

(1) Compensatory damages including but not limited to the cost of credit monitoring services for three years;

(2) Actual damages, including but not limited to plaintiff's bank charges that resulted from the unauthorized debits.

(3) The maximum statutory damages available under 18 U.S.C.§ 2707;

(4) Punitive damages;

(5) Attorneys fees, litigation expenses and costs of suit;

(6) Such other or further relief as the Court deems proper.

COUNT II – ILLINOIS CONSUMER FRAUD ACT

56. Plaintiff incorporates paragraphs 1-42.

57. This claim is brought on behalf of the subclass.

58. Michaels engaged in both unfair and/or deceptive acts and practices, in violation of 815 ILCS 505/2, by:

a. Making the above-quoted representations (paragraph 24) concerning security and privacy of customer information;

b. Failing to properly implement adequate, commercially reasonable security measures to protect their private financial information; and

c. Failing to immediately notify affected customers of the nature and extent of the security breach.

59. These acts and omissions of Michaels were intended to induce plaintiff and the subclass members to rely on the misinformation that their financial information was secure and protected when using debit and credit cards to shop at Michaels.

60. Plaintiff and Illinois subclass members were injured by Michaels' failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while shopping at Michaels.

61. Michaels also engaged in an unlawful practice by failing to comply with 815 ILCS 530/10(a), which provides:

> Sec. 10. Notice of Breach. (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. . . .

62. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act".

63. Michaels' conduct was conducted with reckless indifference toward the rights of others.

WHEREFORE, the Court should enter judgment in favor of plaintiff and the subclass for the following relief:

(1) Compensatory damages;

(2) Punitive damages;

(3) Reasonable attorneys' fees, litigation expenses, and costs of suit;

(4) Injunctive relief; and

(5) Such other or further relief as the Court deems proper.

COUNT III – BREACH OF CONTRACT

64. Plaintiff incorporates paragraphs 1-42.

65. This claim is brought on behalf of the class.

66. Michaels' customers who were interested in making in-store purchases with debit or credit cards were required to provide their card's magnetic strip data and PINs for payment verification.

67. In accepting such financial data, Michaels contracted with plaintiff and members of the class to reasonably safeguard the sensitive, non-public information in accordance with its stated privacy policy (paragraph 24).

68. Under the contract, Michaels was obligated to not only safeguard customer financial information, but also to provide customers with prompt, adequate notice of any security breach or unauthorized access of said information.

69. Michaels breached the contract with plaintiff and members of the class by failing to take reasonable measures to safeguard customer financial data.

70. Michaels also breached its contract with plaintiff and class members by failing to provide prompt, adequate notice of the security breach and unauthorized access of customer financial information by third-party skimmers.

71. Plaintiff and class members suffered and will continue to suffer damages including, but not limited to loss of their financial information, loss of money and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

WHEREFORE, plaintiff requests that the Court enter judgment in favor of plaintiff and the class for the following relief:

(1) Compensatory damages;

(2) Costs of suit;

(3) Such other or further relief as the Court deems proper.

s/ Daniel A. Edelman
Daniel A. Edelman

Daniel A. Edelman
Cathleen M. Combs
James O. Latturner
Catherine A. Ceko
EDELMAN, COMBS, LATTURNER
& GOODWIN, LLC
120 S. LaSalle Street, 18th Floor
Chicago, Illinois 60603
(312) 739-4200
(312) 419-0379 (FAX)

JURY DEMAND

Plaintiff demands trial by jury.

s/ Daniel A. Edelman
Daniel A. Edelman

NOTICE OF LIEN AND ASSIGNMENT

Please be advised that we claim a lien upon any recovery herein for 1/3 or such amount as a court awards. All rights relating to attorney's fees have been assigned to counsel.

s/ Daniel A. Edelman
Daniel A. Edelman

Daniel A. Edelman
EDELMAN, COMBS, LATTURNER
& GOODWIN, LLC
120 S. LaSalle Street, 18th Floor
Chicago, Illinois 60603
(312) 739-4200
(312) 419-0379 (FAX)