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

KIMBERLY M. SIPRUT, on behalf of herself and all others similarly situated, Plaintiff, v. **MICHAELS STORES, INC.**, a Delaware corporation, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Kimberly M. Siprut ("Plaintiff") brings this class action complaint against defendant Michaels Stores, Inc. ("Michaels or Defendant"), on behalf of herself and all others similarly situated, and complains and alleges upon personal knowledge as to herself and her own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

I. NATURE OF THE ACTION

1. On May 5, 2011, Michaels reported that unauthorized hackers obtained highly sensitive financial information of its customers, including debit and credit card information, as well as PIN numbers, by using so-called "skimming devices" on checkout-line swipe terminals at Michaels retail locations.

2. Thus far, Michaels has identified at least 90 terminals that were tampered with in the States of 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.

3. Making matters worse, Michaels first reported the breach almost *three months* after the unauthorized intrusion began. This unnecessary delay has created significantly greater risk that the comprised customer data will be exploited, thus compounding the magnitude and severity of the problem. In fact, Michaels was so slow to recognize the problem and communicate with its customers that some banks – which began spotting suspicious account activity in its own customers' accounts – alerted their customers to the problem before Michaels did.

4. Furthermore, far from taking responsibility for this security breach and owning the gravity of the situation, Michaels has done nothing to remedy the breach or assist consumers who have suffered harm, and who continue to face a real and immediate threat of future harm. In its own words, Michaels simply urges its customers to "protect themselves" and to "seek advice" on how to handle the possibility of their financial information being compromised.

5. Accordingly, in this action, Plaintiff asserts the following claims on her own behalf and on behalf of a proposed class: violation of the Federal Stored Communications Act, negligence, and violation of the Illinois Consumer Fraud Act; and seeks injunctive and declaratory relief, money and statutory damages, and attorneys' fees.

II. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, which confers upon the Court original jurisdiction over all civil actions arising under the laws of the United States, and pursuant to 18 U.S.C. §§ 2520 and 2707. This Court has supplemental jurisdiction over Plaintiff's state statutory claims and common-law claims under 28 U.S.C. § 1367.

7. In addition, this Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of states other than Defendant's state of citizenship.

8. This Court has personal jurisdiction over Defendant because Defendant is registered to do business, and is subject to general jurisdiction, in the State of Illinois. This Court also has personal jurisdiction over Defendant under the Illinois long-arm statute, 735 ILCS 5/2-209, because a substantial portion of the wrongdoing alleged in this Complaint took place in and/or was directed toward the State of Illinois.

9. Venue is proper in this District pursuant to 29 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred here, and because Defendant regularly transacts business in this District and is subject to personal jurisdiction in this District.

III. PARTIES

Plaintiff

10. Kimberly M. Siprut is a resident of the State of Illinois. On or about March 30, 2011, Plaintiff shopped and purchased items at a Michaels retail store location in Mt. Prospect, Illinois. To consummate the purchase, Plaintiff elected to use, and did use, her credit card as her form of payment. On information and belief, Plaintiff's credit card data was stored and was exposed as a result of the security breach of Michaels' swipe terminals.

Defendant

11. Michaels is a Delaware corporation with its principal place of business in Irving, Texas. According to its website, Michaels is North America's largest specialty retailer of arts,

crafts, framing, floral, wall décor, and seasonal merchandise. Michaels currently owns and operates more than 1,045 Michaels stores in 49 states and Canada.

IV. FACTUAL BACKGROUND

The Breach of Michaels' Checkout-Line "Swipe" Terminals

12. Like many other retailers, 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, or to scan a credit card.

13. 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.

14. Between February 8, 2011 and May 6, 2011, an unidentified third party or third-parties tampered with Michaels' payment processing equipment and gained access to the sensitive financial information of thousands of Michaels consumers in at least twenty states.

15. In the wake of this activity, Michaels customers' financial security has been placed at risk, with many Class members reporting having money taken from their bank accounts, often in the amount of $503. The fraud attack has led many banks to freeze bank accounts of customers they think may be vulnerable. For example, Marquette Bank, with 24 branches in the Chicago region, reported that 1,900, or 3 percent, of its customers were identified as potential victims.

16. Michaels failed to employ commercially reasonable security measures, including ensuring the physical security of its checkout line terminals and inspecting and testing its

payment processing equipment, to protect its customers' debit and credit card information during in-store purchases using PIN pads.

17. In addition, Michaels failed to properly implement an intrusion detection and prevention system ("IDPS"). Implementation of an IPDS is a standard practice among companies that collect and retain customer financial and personally identifiable information. Had Michaels properly implemented an IDPS, Michaels would have known of the breach within a reasonable period of time.

18. After the security breach occurred, Michaels further harmed its customers by delaying notifying them for months after the security breach began. As a result, Michaels prevented its customers, including Plaintiff and the other members of the Class, from taking reasonable steps to safeguard or protect their information in a timely fashion.

19. 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.

20. Despite knowing of the data breach for a period of weeks, if not months, Michaels began its May 5, 2011 disclosure letter by saying, "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."

21. In that same letter, Michaels then urged its 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."

22. Thus, Michaels is placing the burden on aggrieved customers 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, nor has Michael's taken any steps to protect or otherwise rectify the damages it has caused Plaintiff and the other members of the Class.

V. CLASS ACTION ALLEGATIONS

28. Plaintiff brings Counts I and II below, on behalf of herself and as a class action, pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All consumers in the United States who made an in-store purchase at a Michaels store in the United States using a debit or credit card that was swiped through a PIN pad at any time from January 1, 2011 through present (the "Class").

Excluded from the Class are Michaels and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the Class; governmental entities; and the judge to whom this case is assigned and any immediate family members thereof.

29. Plaintiff brings Count III, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rules 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure on behalf of a subclass defined as:

> All consumers in the State of Illinois who made an in-store purchase at a Michaels store in the State of Illinois using a debit or credit card that was swiped through a PIN pad at any time from January 1, 2011 through present (the "Illinois Subclass").

Excluded from the Illinois Subclass are Defendant and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the Illinois Subclass; governmental entities; and the judge to whom this case is assigned and any immediate family members thereof. The Class

and Illinois Subclass are collectively referred to as the "Classes," unless specifically indicated otherwise.

30. Certification of Plaintiff's claims for classwide treatment is appropriate because Plaintiff can prove the elements of her claims on a classwide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

31. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Classes are so numerous that individual joinder of all class members is impracticable. On information and belief, there are thousands of consumers who have been damaged by Michaels' wrongful conduct as alleged herein. The precise number of class members and their addresses is presently unknown to Plaintiff, but may be ascertained from Michaels' books and records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

32. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law and fact, which predominate over any questions affecting individual class members, including, without limitation:

a. whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive financial information;

b. whether Defendant properly implemented its security measures to protect customer financial information from unauthorized capture, dissemination and misuse;

c. whether Defendant took reasonable measures to determine the extent of the security breach after it first learned of the breach;

d. whether Defendant's delay in informing consumers of the security breach was unreasonable;

e. whether Defendant's method of informing consumers of the security breach and its description of the breach and potential exposure to damages as a result of the breach was unreasonable;

f. whether Defendant's conduct violates the Stored Communications Act, 18 U.S.C. § 2702;

g. whether Defendant's conduct constitutes negligence;

h. whether Defendant's conduct violates the Illinois Consumer Fraud Act, 815 ILCS 505/1, *et seq.*; and

i. whether Plaintiff and the other Class members are entitled to damages, injunctive relief, or other equitable relief.

33. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform misconduct described above.

34. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Classes because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation; and Plaintiff intends to prosecute this action vigorously. Class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

35. **Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted or refused to act on grounds generally applicable to Plaintiff and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to Class members as a whole.

36. **Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action.

The damages or other financial detriment suffered by Plaintiff and the other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for class members to individually seek redress for Defendant's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By 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.

VI. CLAIMS ALLEGED

COUNT I
Federal Stored Communications Act, 18 U.S.C. § 2702
(On Behalf of the Class)

37. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

38. The Stored Communications Act ("SCA") provides consumers with redress if a company mishandles their electronically stored information, and was designed, among other things, to protect individuals' privacy interests in personal and proprietary information.

39. Section 2702(a)(1) of the SCA provides that "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).

40. 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).

41. Through its payment processing equipment (including its PIN pads), Defendant 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.

42. By failing to take commercially reasonable steps to safeguard sensitive consumer financial data, Defendant 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 Defendants' PIN pads.

43. Section 2702(a)(2)(A) of the SCA provides that "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).

44. 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).

45. An "electronic communications system" is defined by the SCA as "any wire, radio, electromagnetic, photooptical or photoelectronic 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).

46. Defendant 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.

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

48. As a result of Defendant's conduct described herein and its violations of §§ 2702(a)(1) and 2702(a)(2)(A), Plaintiff and the other members of the Class have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft.

COUNT II
Negligence
(On Behalf of the Class)

49. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

50. By agreeing to accept Plaintiff and the other Class members' non-public, sensitive financial information through its payment processing services, Defendant assumed a duty, which

required it to exercise reasonable care to secure and safeguard that information and utilize reasonable methods to do so.

51. Defendant breached its duty of care by failing to provide adequate security, and by failing to protect Plaintiff's and the other Class members' financial data from being captured, accessed, disseminated, and/or otherwise misused by a third party.

52. Defendant also breached its duty of care by failing to provide prompt and clear notification to Plaintiff and members of the Class that their financial data had been compromised.

53. As a direct and proximate result of Defendant's failure to exercise reasonable care and use commercially reasonable security measures, Plaintiff's and the other Class members' financial information and bank account monies were put at risk and/or otherwise stolen.

54. As a direct and proximate result of Defendant's misconduct described herein, Plaintiff and the other Class members have suffered injury in fact through theft of money and/or loss of sensitive financial information and/or the additional costs associated with increased risk of identity theft and monitoring.

55. Plaintiff and the other Class members will continue to incur damages as a result of Defendant's negligence.

COUNT III
Illinois Consumer Fraud Act
(On Behalf of the Illinois Subclass)

56. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

57. At all times relevant hereto, there was in effect in the State of Illinois a statute known as the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2 ("Consumer Fraud Act").

58. Defendant violated the Consumer Fraud Act by failing to properly implement adequate, commercially reasonable, security measures to protect its customers' financial information.

59. Defendant also violated the Consumer Fraud Act by failing to immediately notify affected customers of the nature and extent of the security breach.

60. Defendant's deceptive omissions were intended to induce Plaintiff's and the Illinois Subclass members' reliance on the misinformation that their financial information was secure and protected when using debit and credit cards to shop at Defendant's stores.

61. Plaintiff and the other members of the Illinois Subclass were deceived by Defendant's failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while shopping at Defendant.

62. Plaintiff and other members of the Illinois Subclass have suffered injury in fact, and Illinois Subclass members have lost money and property as a result of Defendant's violations of the Consumer Fraud Act.

63. Plaintiff's and the other Illinois Subclass members' injuries were proximately caused by Defendant's deceptive and/or unfair behavior, which was conducted with reckless indifference toward the rights of others.

VII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class and Illinois Subclass proposed in this Complaint, respectfully requests that the Court enter an Order awarding the following relief:

A. Declaring that this action is a proper class action nationwide, certifying the Class and Illinois Subclass as requested herein, designating Plaintiff as Class and Illinois Subclass Representative and appoint her counsel Class and Illinois Subclass Counsel;

B. Requiring Defendant to pay for not less than three years of credit card fraud monitoring services for Plaintiff and the other members of the Class and Illinois Subclass;

C. An Order awarding actual damages (including punitive damages) as allowable by law;

D. An Order awarding statutory damages to Plaintiff and the other Class and Illinois Subclass members, as provided by the Stored Communications Act;

E. An Order awarding statutory damages to Plaintiff and the other Illinois Subclass members, as provided by the Illinois Consumer Fraud Act;

F. An Order awarding attorneys' fees and costs to Plaintiff and the other members of the Class and Illinois Subclass; and

G. Such other and further relief as may be just and proper.

VIII. JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint so triable.

Dated: June 1, 2011

Respectfully submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC

/s/ Adam J. Levitt
Adam J. Levitt
Edmund S. Aronowitz
55 West Monroe Street, Suite 1111
Chicago, Illinois 60603
Telephone: (312) 984-0000
Facsimile: (312) 984-0001
levitt@whafh.com
aronowitz@whafh.com

Joseph J. Siprut
SIPRUT PC
122 South Michigan Avenue, Suite 1850
Chicago, Illinois 60603
Telephone: (312) 588-1440
Facsimile: (312) 427-1850
jsiprut@siprut.com

William J. Doyle
DOYLE LOWTHER LLP
9466 Black Mountain Road, Suite 210
San Diego, California 92126
Telephone: (619) 573-1700
Facsimile: (619) 573-1701
bill@doylelowther.com

Counsel for Plaintiff

21828