UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

IN RE HANNAFORD BROS. CO. CUSTOMER DATA SECURITY BREACH LITIGATION	)	Docket No. 2:08-MDL-1954 DBH
MAUREEN JOHNSON, of Albany Township, Maine MEL NEVELLS, of Gorham, Maine, BENJAMIN REDMOND, of Durham, Maine LORI VALBURN, of Essex , Vermont, Plaintiffs, v. HANNAFORD BROS. CO., a Maine corporation with its principal place of business at Scarborough, Maine, Defendant.	)	

SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

Plaintiffs above named, on behalf of themselves and all other persons similarly situated, allege on information and belief (except as to paragraphs 35 through 38, which are alleged on the respective Plaintiffs' personal knowledge), including a review of publicly available information and advice of computer security experts, as follows.

Certain plaintiffs named in the actions consolidated in this Consolidated Complaint are not set forth as named plaintiffs here. Those parties do not dismiss any claims or waive any rights. The Plaintiffs named herein are competent to assert the claims set forth herein and can adequately represent the class including all absent class members.

PRELIMINARY STATEMENT

1. This action is brought to obtain redress for losses and damages sustained by the Plaintiffs and other members of the Class (as hereinafter defined) as a result of the failure of the Defendant to maintain the security of private and confidential financial and personal information of Defendant's credit and debit card customers at Hannaford and Sweetbay supermarkets in Maine, New Hampshire, Vermont, Massachusetts, New York and Florida, and at certain independent stores for which the Defendant provided electronic payments services, over a period of approximately three months from December 7, 2007 to March 10, 2008 (the "Class Period").

2. The Plaintiffs were customers of these stores during the Class Period. In the course of making purchases at these stores during the Class Period, Plaintiffs made use of debit cards and credit cards issued by financial institutions to access their bank accounts or create credit relationships.

3. In making these purchases, Plaintiffs and Class members were requested by Defendant to confide and make available to Defendant, its agents and employees, private and confidential debit and credit card information, some of which was encoded on their cards, including their names, card numbers, expiration dates, PIN numbers, and security codes.

4. This information was entrusted to Defendant solely for the purpose of effectuating payment for purchases and with the expectation and implied mutual understanding that Defendant would strictly maintain the confidentiality of the

information and safeguard it from theft or misuse.

5. On or about December 7, 2007, wrongdoers obtained access to Defendant's information technology systems and, until containment of this security breach on or about March 10, 2008, gained access to private and confidential debit card and credit card information, including up to an estimated 4.2 million debit card and credit card numbers, expiration dates, security codes, PIN numbers and other information, belonging to Plaintiffs and other customers of Defendant who had used debit cards and credit cards to transact purchases at supermarkets owned or operated by Hannaford and Sweetbay in the Northeast and Florida and at independently owned grocery stores for which Hannaford provided electronic payments services.

6. As a result of this breach of security, Plaintiffs' and other Class members' debit cards and credit cards were exposed and subjected to unauthorized charges; their bank accounts were overdrawn and credit limits exceeded; they were deprived of the use of their cards and access to their funds; their preauthorized charge relationships were disrupted; they were required to expend time, energy and expense to address and resolve these financial disruptions and mitigate the consequences; and they suffered consequent emotional distress and their credit and debit card information is at an increased risk of theft and unauthorized use.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. §1332(d), because the amount in controversy exceeds $5 million, at least one Plaintiff has citizenship diverse from the Defendant, and there are more than 100 class members.

8. Venue is proper in this Court under 28 U.S.C. §1391(a)(2), because Defendant Hannaford's primary place of business is within this District and the conduct of the Defendant upon which the Plaintiffs' claims are based occurred primarily within this District.

PARTIES

9. Plaintiffs are residents of the following towns and states:

a. Maureen Johnson is a resident of Albany Township, Maine

b. Mel Nevells is a resident of Gorham, Maine

c. Benjamin Redman is a resident of Durham, Maine

d. Lori Valburn is a resident of Essex, Vermont.

10. Defendant Hannaford Bros. Co. ("Hannaford") is a corporation organized under the laws of the State of Maine, with its principal place of business in Scarborough, Maine. Hannaford owns and operates supermarkets in the states of Maine, New Hampshire, Massachusetts, Vermont, and New York.

11. Kash N' Karry Food Stores, Inc. ("Kash N' Karry") is a Delaware corporation, which owns and operates supermarkets in the State of Florida under the name of "Sweetbay".

12. Hannaford and Kash N' Karry are both wholly-owned subsidiaries of Delhaize America, Inc. ("Delhaize"), a Delaware corporation with its principal place of business in North Carolina.

13. During the time periods relevant to this Amended Consolidated Complaint, Hannaford provided information technology and data processing services to Kash N' Karry, including the processing of customer debit card and credit card payments.

14. Hannaford also provided electronic payment processing services to a number of independent stores in various states.

15. Hannaford has stipulated and agreed that judgment may be entered against it based on any liability of Kash N' Karry, Delhaize and such independent stores that may be established in this case. In the interest of simplicity and manageability those entities have not been joined as defendants in this Complaint.

16. The terms "Hannaford" and "Defendant" should be interpreted to include Kash N' Karry, Delhaize, and such independent stores as the context requires.

FACTS

17. On March 17, 2008, Hannaford publicly announced for the first time that between December 7, 2007 and March 10, 2008, the security of its information technology systems had been breached, leading to the theft of as many as 4.2 million debit card and credit card numbers belonging to individuals who had made purchases

at more than 270 of its stores, including 165 Hannaford stores in New England and New York, 106 Sweetbay stores in Florida and an additional number of independent grocery stores for which Hannaford provided electronic payment services in various states, and that it had already received reports of approximately 1,800 cases of fraud resulting from the theft of those numbers.

18. For some period of time before, during and after the Class Period Defendant has invited customers, including Plaintiffs and the Class members, to make use of their debit cards and credit cards to pay for purchases at Hannaford supermarkets and other stores for which Hannaford provided electronic payment services.

19. Based on this invitation Plaintiffs and the Class members made use of their debit cards and credit cards to pay for their purchases at such stores during the Class Period.

20. In the course of making such purchases and paying for them, Class members confided their private and confidential debit card and credit card information to Defendant solely for the purpose of enabling Defendant to effectuate such payments. Such data was confided based on express and implied representations by Defendant and on the expectation and implied mutual understanding that the data confided would be protected and safeguarded from access by unauthorized individuals.

21. During the Class Period, Defendant failed to adequately safeguard and protect the private and confidential debit card and credit card information of Plaintiffs

and Class members, so that wrongdoers were able to obtain access to such data within Defendant's information technology systems or in the course of transmission of the data to financial institutions.

22. Lack of adequate security in Defendant's information technology systems enabled the wrongdoers to place foreign software, known as malware, on Defendant's information technology systems, which then provided the wrongdoers with access to customer debit card, credit card, and possibly other electronic information then in transit or temporarily stored on the system, and then diverted this information to the wrongdoers.

23. Defendant did not monitor their information technology system for the presence of foreign software in a manner that would enable them to detect this intrusion, so that the breach of security and diversion of customer information was able to continue unnoticed for more than three (3) months.

24. Defendant' information technology system had multiple security shortfalls, including:

a. lack of proper monitoring solutions;

b. failure to encrypt internal network traffic flowing between store and processor;

c. point-of-sales systems that were open to attack;

d. insecure wireless connections; and/or

e. remote access deficiencies.

25. On February 27, 2008, Visa notified Hannaford that a pattern of unusual

fraudulent credit card activity involving customers who had made debit card and credit card transactions at Hannaford stores indicated that its information technology system had been breached.

26. On March 8, 2008, Hannaford computer technicians discovered the means by which wrongdoers had obtained unauthorized access to confidential customer data in its system.

27. The security breach was not contained until March 10, 2008. On that day, Defendant notified certain financial institutions of the data intrusion.

28. Although Defendant first became aware of the breaches of its information technology system as early as February 27, 2008, Defendant failed to disclose publicly that customers' private and confidential financial and personal information had been accessed and stolen until Hannaford announced the data intrusion publicly on March 17, 2008.

29. The wrongdoers who obtained such access and stole customers' data and their transferees misused this data by making unauthorized charges against the debit card and credit card accounts of Plaintiffs and other Class members. By the time Hannaford publicly announced the security breach, over 1,800 such charges had already been identified. Since then many more have taken place.

30. Defendant's initial public disclosure of the theft of its customer's personal and financial data was incomplete. In "[a] Message From Hannaford CEO Ron Hodge" posted on its website on March 17, 2008, Hannaford stated:

> Hannaford has contained a data intrusion into its computer network that resulted in the theft of customer credit and debit card numbers. No personal information, such as names or addresses, was accessed. Hannaford doesn't collect, know or keep any personally identifiable customer information from transactions.

31. Hannaford's initial posting failed to disclose that additional information including card expiration dates and security codes as well as positive authorization results had been stolen or that this information was sufficient to enable the wrongdoers to make fraudulent charges to cardholder accounts. The initial posting also failed to disclose that as of the time Hannaford became aware of the theft over 1,800 fraudulent charges had been identified and that many more could be expected. The initial posting failed to disclose the time period during which customer data was exposed to theft, the number of customers affected, or the independent stores whose customers' data had been implicated in the breach.

32. Defendant's notification to its customers concerning the theft of their data was limited to the initial announcement, postings on its website, and notices posted in its stores. Defendant has not attempted to notify its customers individually through their card issuing financial institutions nor has it undertaken any public advertising campaign calculated to reach its customer base in the various states in which it does business.

33. Defendant still has not advised each of its customers of exactly what private and confidential financial and personal information belonging to each of them was stolen or exposed to theft as a result of this data breach. Nor has Defendant taken

any other steps to assist customers whose credit and debit card data was stolen by provision of credit or card monitoring, reimbursement of out of pocket expenses, or compensation for time, effort, disruption and emotional distress occasioned by the breach of its information technology system.

34. Following Hannaford's announcement of the data breach:

a. some financial institutions immediately cancelled customers' debit and credit cards and issued new cards, while others waited for evidence of unauthorized activity to take action;

b. financial institutions which did not immediately cancel customers' cards monitored customer accounts for unusual activity and cancelled cards immediately upon being aware of apparent fraudulent charges or attempts to make apparently fraudulent charges, in many cases without the knowledge of the customer.

c. customers suffered unauthorized charges to their debit card and credit card accounts;

d. customers' accounts were overdrawn and their credit limits exceeded by virtue of unauthorized charges;

e. customers were deprived of use of their cards for appreciable periods of time and were unable to access their accounts or their funds;

f. customers lost accumulated miles and points toward bonus

awards and were unable to earn points during the interval their cards were inactivated;

g. customers who requested that their cards be cancelled were required to pay fees to issuing banks for replacement cards;

h. customers who had registered their cards with online sellers were required to cancel and change their registered numbers;

i. customers who had given creditors pre-authorization to charge their debit cards or credit cards for recurring payments were required to change the pre-authorizations;

j. customers were placed in non-payment status by virtue of their cards being overdrawn or abruptly cancelled and were required to pay penalties and service reinstatement fees;

k. customers purchased identity theft insurance and credit monitoring services to protect themselves against possible consequences of the breach; .

l. customers suffered emotional distress as they were forced to cope with the unauthorized charges and other consequences of Defendant's' data breach, and some customers are still not aware of the data breach or that their data has been compromised.

SPECIFIC REPRESENTATIVE PLAINTIFF ALLEGATIONS.

35. During the Class Period Plaintiff Maureen Johnson and her fiance, Randall Butters, maintained a joint deposit account at Key Bank, which they accessed with debit cards issued by the bank. Both Ms. Johnson and Mr. Butters shopped at a Hannaford supermarket in Norway, Maine during the Class Period and used their Key Bank debit cards to make purchases there. On or about March of 2008 they learned that fraudulent charges totaling more than $800 had been made to the joint account using Mr. Butters' debit card number. They protested the fraudulent charges and cooperated with their bank, the California vendors where some of the fraudulent charges had been made, and with the State Police. They applied for and received a loan from Key Bank to cover the amounts of the charges pending Key Bank's investigation. Key Bank ultimately reinstated the fraudulent charges and advised Ms. Johnson and Mr. Butters that the charges had likely resulted from the Hannaford Bros. data security breach. The bank cancelled Mr. Butters' card immediately because the card experienced fraud charges. Ms. Johnson requested that the bank also cancel her card. The bank cancelled her card, then reissued new cards with different numbers to each of them, and charged each of them a fee of $5.00 for the new cards. The $5.00 fee for Mr. Butters' card was reversed by the bank. The $5.00 fee for Ms. Johnson was not reversed, despite her request for a fee reversal.

36. Plaintiff Mel Nevells used his Discover Credit card at a Hannaford store in Standish, Maine during the Class Period. When he learned of the data security breach and that his confidential account access information had been stolen, he

purchased identity theft insurance through Discover for at least three months at a cost of $12.99 per month to protect himself from the consequences of misuse of his card number.

37. Plaintiff Benjamin Redmond used his Key Bank debit card to make purchases at a Hannaford Shop N' Save Store in Newport Maine during the Class Period. In early 2008 he tendered the card to make a purchase at a Dunkin Donuts store in Lewiston, Maine but the card was refused. He logged on to check the state of his account, and received a message that he should get in touch with the bank at once. When he did so, he was told that over $3,000 in fraudulent charges had been made on the card in Mexico. The card was cancelled and the bank advised that a new card would be forthcoming in 7-10 days in the ordinary course or within 3-4 days upon payment of an expedited delivery fee of $15-25. Mr. Redmond paid the expedited delivery fee in order to receive the replacement card promptly. He also paid a lost card fee of $5.00 in connection with the cancellation and replacement of his card.

38. Plaintiff Lori Valburn used her debit and credit cards issued by the Vermont State Employees Credit Union and her Discover Card credit card to make purchases at Hannaford stores near Burlington, Vermont during the Class Period. In April 2008, she reviewed her Discover Card statement and learned that an unauthorized cash withdrawal for $500.00 had been made against her account on March 19, 2008 in Indiana. She called the issuers of all her cards and had them cancelled and replaced. She also spoke with the fraud unit at Discover Card. She was without her canceled cards for approximately 7-10 days. Due to the uncertainty and

threat of further unauthorized use of her accounts, she purchased identity theft insurance through Discover Card at a cost of $2.99 per month and has continued to pay the monthly premium of $2.99 to the present day.

INJURY AND DAMAGES

39. As a direct and proximate result of Hannaford's failure to maintain the security of its customers' private and confidential financial and personal data, Plaintiffs and Class members suffered a disruption of their financial affairs and endangerment of their financial assets and resources. They have had to expend time, effort and money to address, correct, repair, and/or mitigate the consequences of the disruption of their financial affairs and to mitigate and avert the harm threatened to their financial assets and resources, including their credit reputations. They have incurred out-of-pocket loss and damage. They have experienced emotional distress. They remain exposed to the risk of fraud in cases in which compromised debit and credit cards have not been cancelled.

40. The out-of-pocket expenditures by the Plaintiffs and Class members in mitigation of the harm caused by Hannaford's negligence and breach of contract include, but are not limited to:

a. fees paid by customers who sought to cancel their cards and obtain replacement cards to protect themselves from potential unauthorized charges;

b. fees to purchase credit reports, to arrange for credit monitoring,

and to purchase identify theft and overdraft insurance;

CLASS ACTION ALLEGATIONS

41. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3) on behalf on themselves and all other persons similarly situated.

> The Class consists of all persons or entities anywhere in the United States, who made purchases at stores owned or operated by Defendant during the period from December 7, 2007 through March 10, 2008, using debit or credit cards, whose debit or credit card numbers, expiration dates and/or security codes were accessed in the course of an electronic breach of Defendant's data security, and who made out of pocket expenditures in mitigation of the consequences to them of such data security breach, including, but not limited to payment of fees to obtain prompt replacement of cancelled cards and purchase of credit monitoring and identity theft insurance.

42. The Class does not include the Court, the U.S. Magistrate Judge, counsel for any party, any of their employees or immediate family members, the Defendant, any director, officer or employee of the Defendant, or any of their immediate family members.

43. The exact number of Class members and their identities are unknown at this time. However, since as many as 4.2 million debit card and credit card numbers of Defendant' customers were stolen, the Class members are so numerous that joinder of all individual Class Member is impracticable.

44. Questions of law and fact common to all Class members predominate over any questions affecting only individual members, including the following:

i. Whether Defendant acted negligently in failing to properly safeguard Class

members' financial and personal data;

ii. Whether Defendant breached express or implied contracts with Class members by failing properly to safeguard their private and confidential financial and personal data and by failing to notify them of the breaches of its computer data systems and the nature and extent of their data that had been stolen as soon as practicable after such breaches were discovered;

45. Plaintiffs' claims are typical of the claims of all Class members, because all such claims arise from the same set of facts regarding Defendant's failures:

i. to protect Plaintiffs' and Class members' private and confidential financial and personal data;

ii. to discover and remediate the security breach of their computer systems more quickly; and

iii. to disclose to Plaintiffs and Class members in a complete and timely manner information concerning the security breach and the theft of their private and confidential financial and personal data.

46. Plaintiffs have no interests that are antagonistic to the interests of other Class members.

47. Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel for the prosecution of this case as a class action.

48. Defendant has acted and refused to act on grounds that apply generally to the Class, so that injunctive or declaratory relief is appropriate respecting the class as a whole.

49. This class action is superior to other available methods for fairly and efficiently adjudicating Class members' claims because:

a. the class is readily definable and prosecution of this action as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual cases;

b. the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications, which could establish incompatible standards of conduct for the Defendant or allow some Class members' claims to affect adversely other Class members' abilities to protect their interests;

c. this forum is an appropriate one in which to concentrate the litigation since Hannaford is located here and its conduct giving rise to Plaintiffs' and Class members' claims occurred here; and

d. the case is manageable as a class action.

COUNT I – BREACH OF IMPLIED CONTRACT

50. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 49 as if fully set forth herein.

51. When they confided their private and confidential debit card and credit card information to Defendant in order to make purchases at Defendant's stores, Plaintiffs and Class members entered into implied contracts with Defendant under

which Defendant agreed to safeguard and protect all such information and to notify them that the confidentiality of such information was compromised.

52. Plaintiffs and Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract with Defendant.

53. Defendant breached the implied contracts they had made with Plaintiffs and Class members by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information.

54. The damages sustained by Plaintiffs and Class members as described above were the direct and proximate result of Defendant's breaches of these implied contracts.

COUNT II - NEGLIGENCE

55. Plaintiffs repeat and reallege the allegations in paragraphs 1 through 49 as if fully set forth herein.

56. Defendant owed its customers a duty of care in the handling and safeguarding of their private and confidential financial and personal information entrusted to them for the purpose of making purchases at its stores.

57. Defendant breached its aforesaid duty to use due care to safeguard the private and confidential financial and personal information entrusted to it by Plaintiffs and Class members. Their breaches included, but are not limited to, the following:

a. failing to monitor their IT network for the presence of foreign

software in a manner that would enable them to detect this intrusion, so that the breach of security and diversion of customer information was able to continue undetected for more than three (3) months;

b. failing to encrypt internal network traffic flowing between store and processor, running point-of-sales systems that were open to attack, maintaining insecure wireless connections and/or having remote access deficiencies;

c. failing to secure its internal network credit and debit card authorization traffic from access by malware implanted on its network;

d. failing to take appropriate steps to identify and contain the security breach when it was first discovered; and

e. failing to appropriately limit employee access.

58. The damages described above were the direct and proximate result of Defendant' breaches of their duty use due care to safeguard the private and confidential financial and personal information entrusted to them by Plaintiffs and Class members.

PRAYERS FOR RELIEF

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the members of the Class, respectfully request that the Court:

A. certify this action as a class action for the purposes of final injunctive relief pursuant to Fed. R. Civ. P. 23(a) and (b)(2), and for damages pursuant to

Fed. R. Civ. P. 23(a) and (b)(3), and appoint Plaintiffs as Class Representatives and their counsel as Class Counsel thereof.

B. enter judgment awarding damages to Plaintiffs and Class members for their out of pocket expenditures made in mitigation of the harm caused by Defendant's negligence or breach of contract;

C. award attorneys' fees, expenses, interest and the costs of suit; and

D. award such other and further relief as it may deem just and appropriate.

JURY TRIAL DEMAND

Plaintiffs, on behalf of themselves and the Class, demand a jury trial on all issues so triable.

Dated: June 5, 2012.

s/ Peter L. Murray
Peter L. Murray (Maine Bar No. 1135)

s/ Thomas C. Newman
Thomas C. Newman (Maine Bar. No. 2199)

MURRAY, PLUMB & MURRAY
75 Pearl Street
Portland, ME 04101
Tel: (207) 773-5651

s/Lewis Saul
Lewis Saul (New York Bar No. 4468740)

LEWIS SAUL & ASSOCIATES P.C.
183 Middle Street, Suite 200
Portland, ME 04101
Tel: (207) 874-7407

Interim Plaintiffs' Lead Counsel

s/ Samuel E. Lanham
Samuel E.Lanham (Maine Bar No. 2258).

LANHAM BLACKWELL, P.A.
470 Evergreen WOods
Bangor, ME 04401
207 942-2898

Associate Interim Plaintiffs' Lead Counse