



Fraudulent activity has occurred on some of those cards.

### **JURISDICTION AND VENUE**

3. Jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1332(d)(2) because the matter in controversy exceeds \$5 million, at least one Class member has diverse citizenship from Defendant, and there are more than 100 Class members.

4. Venue properly lies in this District pursuant to 28 U.S.C. § 1391(a)(2) because this is the judicial district in which a substantial part of the events giving rise to the claims occurred.

### **PARTIES**

5. Plaintiff Moises Merino resides in California. Plaintiff received a letter from his card-issuing bank, Bank of America, in mid-January 2009 informing him that his debit card information was “compromised.” This was the first time Bank of America notified him of a compromise or data breach since he opened his account in approximately 1994. On information and belief, Plaintiff’s card was compromised from the Heartland breach.

6. Defendant Heartland Payment Systems, Inc. is incorporated in Delaware. Its headquarters are located at 90 Nassau Street, Princeton, NJ, 08542. According to its website, Heartland is “one of the nation’s largest payment processors delivering credit/debit/prepaid card processing . . . solutions.” Heartland services more than 150,000 merchant locations nationwide.

### **OPERATIVE FACTS**

7. On January 20, 2009, Heartland issued a press release and established a website, [www.2008Breach.com](http://www.2008Breach.com), stating:

- Heartland was notified by Visa and MasterCard of suspicious activity

surrounding card transactions that Heartland processed.

- Heartland “uncovered malicious software that compromised data, which crossed the company’s network in 2008.”
- Heartland “advises cardholders to examine their monthly statements closely and report and suspicious activity to their card issuers.”

8. According to several media reports, including a report in The Washington Post, 100 million card numbers may have been affected by the breach. That figure would make the breach one of the largest data breaches ever reported.

9. On January 20, 2009, The New York Times reported the following:

Robert H. B. Baldwin Jr., Heartland’s president and chief financial officer, said that his company believed the card numbers, expiration dates, and in some cases cardholder names were exposed after attacks on its computer systems at the one point where data had been unencrypted.

Once consumers swiped their cards, so-called sniffer software captured that data as Heartland sought authorization from the major payment companies and banks. Customers of Visa, MasterCard, American Express and Discover Financial were all vulnerable.

....

Data thieves introduced the software as early as May [2008], but Heartland did not detect the breach until it was alerted to the activity in late fall [2008].

....

Heartland . . . processes about 100 million transactions a month.

10. On January 20, 2008, The Wall Street Journal reported that “the data the criminals accessed - called ‘track data’ in the industry - are the equivalent of the crown jewels since criminals can use the information to make fake cards.”

11. According to several media reports, including a report in The Washington Post, fraudulent activity has begun to occur on some of the compromised cards.

12. Heartland failed to contain the breach for several months. The breach began as early as May 2008. Visa and Mastercard reportedly alerted Heartland to suspicious card activity in late fall 2008. However, Heartland did not locate and contain the malicious software for several more months. On January 20, 2009, Heartland disclosed on its website that “last week [mid-January 2009], the investigation uncovered malicious software.”

13. The fact that several months passed between when the breach began in May 2008 and when Heartland was first alerted to suspicious activity in late fall 2008 casts doubt on Heartland’s security measures and intrusion detection systems. Perhaps even more alarming is the fact that malicious software remained on Heartland’s network until several months after Visa and Mastercard alerted Heartland to suspicious card activity.

14. Heartland’s delay in detecting, containing, and announcing the breach harmed Class members. Had the breach been contained sooner, fewer card numbers would have been compromised. Also, had the breach been announced sooner, Class members would have had more time to take protective measures to prevent fraud.

15. Heartland was familiar with industry-wide duties and standards regarding data security. In its December 31, 2007 Form 10-K filed with the Securities and Exchange Commission, Heartland disclosed that it must comply with a variety of data security standards including: (i) Payment Card Industry Data Security Standards (PCI-DSS); (ii) “ANSI standards that are published as the ‘ASC X9 TG-3 PIN Security Compliance Guideline’”; (iii) “SAS-70” reviews; (iv) “Cyber-Risk Assessments”; and (v) “industry standards and best practices

established by regulatory guidelines.” See Form 10-K pg. 23, 30.

16. Heartland also disclosed the following in the Risk Factor section of its Form 10-K: “Our computer systems could be penetrated by hackers and our encryption of data may not prevent unauthorized use. . . . [O]ur agreements with financial institutions require us to take certain protective measures to ensure the confidentiality of merchant and consumer data.” See Form 10-K pg. 27.

17. Heartland also noted on its website that it is obligated to provide “secured transactions.” See <http://www.heartlandpaymentsystems.com/affiliate/mbor.asp>.

18. On information and belief, Heartland failed to comply with one or more applicable data security standards.

19. As a result of Heartland’s inadequate data security, Class members suffered or risk suffering damages, including but not limited to:

a. out-of-pocket losses for, *inter alia*: (i) fraudulent charges on their cards, to the extent not reversed by banks; (ii) fees imposed by certain banks for obtaining replacement cards; (iii) costs to order new checks for new checking accounts; (iv) costs for credit monitoring, identity theft insurance, and related products; and (v) unpaid time off from work responding to the breach;

b. the time and burden of: (i) closely scrutinizing past and future account statements for fraud; (ii) formally disputing fraudulent activity with banks; (iii) reporting fraudulent activity to the police, Federal Trade Commission, or other third parties; (iv) cancelling compromised cards; (v) activating replacement cards; and (vi) re-establishing electronic payment links from old card numbers to new card numbers;

- c. loss of use of credit and debit cards while old cards are cancelled and new cards are issued;
- d. fear, anxiety, and apprehension of fraud or loss of money;
- e. loss of time spent seeking to prevent or undo harm; and
- f. other economic and non-economic damages.

20. The Class is also entitled to injunctive relief, including but not limited to the requirement that Heartland enhance the security of its payment processing systems to contain the intrusion and/or minimize the likelihood of future intrusions. Injunctive relief is required because money damages alone are insufficient to redress the irreparable harm that Class members face absent these injunctive measures.

#### **CLASS ACTION ALLEGATIONS**

21. Plaintiff brings this class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of himself and all others similarly situated (the “Class”), defined as follows:

All persons or entities in the United States whose credit or debit card information was stolen or compromised from Heartland Payment System, Inc.’s payment processing network.

Excluded from the Class are Heartland and its officers and directors.

22. The Class is so numerous that joinder of all Class members is impracticable. The breach reportedly involved up to 100 million credit and debit card accounts.

23. Heartland’s conduct in failing to safeguard Class members’ card data was uniform among the Class.

24. Questions of law and fact common to the Class predominate over questions affecting only individual Class members. Questions of law and fact common to the Class include

but are not limited to:

- a. whether Heartland owed a duty to Class members and breached that duty regarding data security;
- b. whether Heartland breached implied contracts regarding data security;
- c. whether Heartland breached contracts regarding data security to which Class members were third party beneficiaries;
- d. whether Heartland violated the New Jersey Consumer Fraud Act, N.J. Stat. § 56:8-2 *et seq.*, when failing to safeguard Class members' card data;
- e. whether Heartland violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*; and
- f. whether Class members have suffered legally cognizable damages from Heartland's conduct.

25. Plaintiff's claims are typical of the claims of all Class members. The claims of Plaintiff and the Class arise from the same set of facts regarding Heartland's failure to protect card data.

26. Plaintiff maintains no interests that are antagonistic to the interests of other Class members.

27. Plaintiff is committed to the vigorous prosecution of this action and has retained competent counsel experienced in prosecuting class actions of this type. Plaintiff is an adequate representative of the Class and will fairly and adequately protect the interests of the Class.

28. A class action is a fair and efficient method of adjudicating the claims of Plaintiff and the Class for the following reasons:

- a. Common questions of law and fact predominate over any question affecting any individual Class member;
- b. Litigating separate non-class actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members. That would establish incompatible standards of conduct for Heartland or allow some Class members' claims to adversely affect other Class members' ability to protect their interests;
- c. Plaintiff anticipates no difficulty in the management of this litigation as a class action;
- d. The Class is readily definable; and
- e. Prosecution 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 complex litigation.

29. For these reasons, a Class action is superior to other available methods for the fair and efficient adjudication of this controversy.

#### **COUNT I: NEGLIGENCE**

30. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

31. Heartland assumed a duty, and had duties imposed by industry standards, to use reasonable care to secure Class members' credit and debit card information. By its acts and omissions, Heartland unlawfully breached these duties. The Class was damaged thereby.

32. Heartland was familiar with industry-wide duties and standards regarding data security as set forth above.

33. Heartland knew or should have known that its computer system for processing Class members' card information was not secure.

34. The compromise of Class members' card information, and the resulting out-of-pocket loss, burden, fear, anxiety, apprehension of fraud or loss of money, loss of time spent seeking to prevent or undo harm, and other economic and non-economic damages were the direct and proximate result of Heartland's breach of its duties.

**COUNT II: BREACH OF IMPLIED CONTRACTS**

35. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

36. Plaintiff and the Class entered into implied contracts with Heartland when engaging in card transactions using Heartland's payment processing system.

37. Heartland impliedly agreed to take appropriate measures to safeguard Class members' card information.

38. The implied contracts were based on, among other things, Heartland's website and Form 10-K, which noted the existence of data security obligations and standards.

39. Heartland breached its implied contracts by failing to adhere to applicable data security standards or otherwise maintain adequate data security.

40. As a result of these breaches, Plaintiff and the Class have been damaged.

**COUNT III: BREACH OF CONTRACTS TO WHICH  
PLAINTIFFS WERE THIRD PARTY BENEFICIARIES**

41. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

42. Plaintiffs are intended third party beneficiaries of contracts entered into between

Defendant and third parties including but not limited to Defendant's merchant clients.

43. Defendant's contracts with third parties required that Defendant take appropriate steps to safeguard Plaintiffs' credit card information.

44. Defendant breached those contracts.

45. As a result of the breaches, Plaintiff and the Class have been damaged.

**COUNT IV: VIOLATION OF THE  
NEW JERSEY CONSUMER FRAUD ACT,  
N.J. STAT. § 56:8-2 ET SEQ.**

46. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

47. Heartland's conduct alleged above, including but not limited to: (i) failing to adhere to data security standards; (ii) failing to safeguard Class members' card information; (iii) expressly or impliedly misrepresenting that it complied with applicable data security standards; and/or (iv) concealing from Class members that its data security measures were deficient, constituted violations of N.J. Stat. § 56:8-2 *et seq.*

48. Plaintiff and the Class are entitled to treble damages and recovery of attorneys' fees and litigation costs pursuant to N.J. Stat. § 56:8-19.

**COUNT V: VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")**

49. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

50. The Fair Credit Reporting Act ("FCRA") imposes the following duty: "Every consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under [15 U.S.C. § 1681b]." 15 U.S.C. §

1681e(a). Section 1681b sets forth various permissible purposes for the furnishing of consumer reports. Allowing consumer information to be accessed by a computer hacker does not comply with any permissible purpose set forth in Section 1681b.

51. The FCRA defines “consumer reporting agency” as follows:

The term “consumer reporting agency” means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of *furnishing consumer reports to third parties*, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f) (emphasis added).

52. The FCRA defines “consumer report” as follows:

The term “consumer report” means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, *credit capacity*, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of *servicing as a factor in establishing the consumer’s eligibility for*

(A) *credit* or insurance to be used primarily for personal, family, or household purposes;

(B) employment purposes; or

(C) any other purpose authorized under [15 U.S.C. §1681b].

15 U.S.C. §1681a(d)(1) (emphasis added).

53. Heartland is a “consumer reporting agency” as defined by the FCRA. Heartland assembles credit and debit card information and furnishes it to numerous third parties including Visa, Mastercard, and card-issuing banks.

54. Credit and debit card information constitutes a “consumer report” as defined by the FCRA. Card information is used at the point of sale to determine cardholders’ credit capacity

- *i.e.*, their eligibility to purchase goods or services.

55. Class members are “consumers” as defined and construed under the FCRA, 15 U.S.C. §1681a(c).

56. Heartland received fees for assembling and furnishing consumer information.

57. The FCRA also requires “any person that maintains or otherwise possesses consumer information . . . derived from consumer reports for a business purpose to properly dispose of any such information or compilation.” 15 U.S.C. § 1681w(a)(1). In connection with this rule, several disposal provisions are codified at 16 C.F.R. §§ 682.1 to 682.5. Those provisions state the following, in relevant part:

- “Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.” 16 C.F.R. § 682.3(a).
- The term “dispose” is defined to include the “transfer of any medium, including computer equipment, upon which consumer information is stored.” 16 C.F.R. § 682.1(c)(2).
- The term “consumer information” is defined to include “any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report.” 16 C.F.R. § 682.1(b).

58. Defendant’s processing of card transactions met the definition of “disposal” because Defendant transferred cardholder data.

59. The credit and debit card information that Defendant processed was consumer information for purposes of the disposal rule.

60. Defendant failed to comply with the disposal rule because Defendant did not take reasonable measures to protect against unauthorized access.

61. Defendant willfully or recklessly failed to comply with the FCRA. Defendant knew or recklessly disregarded that its data security was inadequate when processing Plaintiff's card transactions.

62. Defendant willfully or recklessly failed to properly: (i) monitor for unauthorized access to cardholder information; and/or (ii) adopt procedures to prevent or detect unauthorized access to cardholder information.

63. The FCRA states the following with respect to damages:

(a) Any person who willfully fails to comply with any requirement imposed under this title with respect to any consumer is liable to that consumer in an amount equal to the sum of

(1)(A) any actual damages sustained by the consumer as a result of the failure or damages of not less than \$100 and not more than \$1,000

....

(B) such amount of punitive damages as the court may allow; and

(C) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

15 U.S.C. § 1681n(a).

64. Plaintiffs have been damaged by Defendant's inadequate data security. Plaintiffs are entitled to actual damages or statutory damages of not less than \$100 and not more than \$1,000, as well as punitive damages, litigation costs, and attorney's fees.

65. The FCRA also imposes liability for negligent as opposed to willful violations.

The FCRA states:

(a) Any person who is negligent in failing to comply with any requirement imposed under this title with respect to any consumer is liable to that consumer in an amount equal to the sum of

(1) any actual damages sustained by the consumer as a result of the failure; and

(2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

15 U.S.C. § 1681o(a).

66. To the extent Defendant is found to have negligently failed to comply with the FCRA, Plaintiffs are entitled to actual damages, as well as litigation costs and attorney's fees.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, respectfully requests the following relief:

A. that this Court certify this action as a Class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint Plaintiff and his counsel to represent the Class;

B. that this Court enter judgment in favor of Plaintiff and the Class, and against Defendant under the legal theories alleged herein;

C. that this Court award damages to Plaintiff and the Class under the legal theories alleged herein;

D. that this Court award injunctive relief, including but not limited to the requirement that Defendant enhance the security of its payment processing systems to contain the intrusion and/or minimize the likelihood future intrusions;

E. that this Court award attorneys' fees and costs of the suit;

F. that this Court award mandated treble damages pursuant to N.J. Stat. §

56:8-19;

G. that this Court award statutory damages, punitive damages, costs of the suit, and attorneys' fees pursuant to the FCRA;

H. that this Court award pre-judgment and post-judgment interest at the maximum rate allowable by law; and

I. that this Court award such other relief as it may deem just and appropriate.

**JURY TRIAL DEMAND**

Plaintiff demands a trial by jury on all issues so triable.

Dated: January 29, 2009

Respectfully Submitted,

s/ Lisa Rodriguez  
TRUJILLO, RODRIGUEZ & RICHARDS, LLC  
Lisa J. Rodriguez  
258 Kings Highway East  
Haddonfield, NJ 08033  
Tel: (856) 795-9002  
Fax: (856) 795-9887

*Liaison Counsel for Plaintiff and the Class*

BERGER & MONTAGUE, PC  
Sherrie R. Savett  
Michael T. Fantini  
Jon Lambiras  
1622 Locust Street  
Philadelphia, PA 19103  
Tel: (215) 875-3000  
Fax: (215) 875-4604

*Counsel for Plaintiff and the Class*

SHELLER, P.C.

Jamie Sheller  
1528 Walnut St., 3rd Floor  
Philadelphia, PA 19102  
Tel: (215) 790-7300  
Fax: (215) 546-0942

*Counsel for Plaintiff and the Class*

malta456269-001.wpd