



(collectively, “Payment Cards”) (*a.k.a.*, “Issuers”), (ii) acquire merchants who accept Payment Cards (*a.k.a.*, “Acquirers”), or (iii) both.

2. Defendants are members of the Associations. On information and belief, Defendants are both Issuers and Acquirers. At all relevant times, Defendants maintained (and continue to maintain) credit card merchant processing programs (the “Programs”), pursuant to which Defendants provide processing and *related* services for merchants which accept, as a method of payment *for goods and services*, Payment Cards and other proprietary credit cards and/or debit cards approved for acceptance by Defendants.

3. At all relevant times, Defendants contracted with Heartland Payment Systems, Inc. (“Heartland”) for Heartland to serve as their agent to provide various services related to the Programs including, without limitation, risk management, front-end and back-end processing and merchant chargebacks. At all relevant times, under the contracts between Defendants and Heartland, Heartland also acted as their agent to process transactions that utilized Payment Cards “issued” by Plaintiffs.

4. At all relevant times, Defendants also contracted with Heartland for Heartland to serve as their agent to provide them with “Acquirer” services, thereby serving as Defendants’ *de facto* Acquirer entity. As part of its Acquirer services, among other things, Heartland performed the initial underwriting to determine a merchant’s eligibility to participate in, and process transactions through, the Networks established by the Associations. Heartland is not and cannot be a member of the Associations—principally because it is not a financial institution—but rather, was and is “sponsored” into the Associations by its principals, KeyBank and Heartland Bank. This “sponsorship” allows Heartland access to the Networks in its capacity as Defendants’ agent.

5. Heartland has admitted in its filings with the Securities and Exchange Commission (“SEC”) that its KeyBank sponsorship permits it to “route Visa and MasterCard transactions under (KeyBank’s) control and identification numbers to clear credit bank card transactions through Visa and MasterCard . . . (and) enables (Heartland) to settle funds between the cardholders and merchants by delivering funds to (KeyBank), which in turn transfers settlement funds to the merchants’ bank accounts.” On information and belief, this is also true with respect to Heartland’s business relationship with Heartland Bank.

6. Heartland is a publicly traded corporation on the New York Stock Exchange (symbol: HPY), is reportedly the fifth largest payment processor in the United States, and claims to be the ninth largest payment processor in the world. Heartland processes Payment Card transactions and provides other financial services for over 250,000 merchants across the United States, including restaurants and retail stores, most of which is done pursuant to its principal/agent and contractual relationships with Defendants. Heartland processes approximately one hundred million (100,000,000) Payment Card transactions per month, totaling over eighty billion dollars (\$80,000,000,000) worth of transactions per year.

7. In connection with the Payment Card processing operations it conducts pursuant to its agreements with and “sponsorship” by Defendants, Heartland comes into the possession of—and is entrusted with—confidential personal and financial information of millions of consumers conducting business with Defendants’ merchant customers. Heartland—through, among other things, its agreements with Defendants and its sponsored admission to the Associations—is obligated to the members of the Associations—including Plaintiffs—to possess and employ the particularized knowledge, skills and Payment Card processing system safeguards to protect such confidential personal and financial information (hereafter referred to as the

“Confidential Payment Card Data”). As Heartland’s “sponsor” and principal, Defendants also are obligated to their fellow members of the Associations—including Plaintiffs—to, among other things, monitor, audit, oversee and confirm that Heartland’s Payment Card processing system safeguards are adequate, comply with all applicable laws and guidance, are in place, are being properly monitored, managed, updated and maintained, and are fully operational, all in order to protect Confidential Payment Card Data.

**8.** Notwithstanding the above obligations of Heartland, KeyBank and Heartland Bank, beginning at least as early as December 26, 2007, unauthorized persons accessed Heartland’s unsecure Payment Card processing system, resulting in the loss of Confidential Payment Card Data associated with approximately one hundred thirty million (130,000,000) Payment Cards (the “Data Breach”).

**9.** The Data Breach occurred because, among other reasons, (i) Heartland’s management, through cost-cutting and cost avoidance, made conscious business decisions, ratified and/or approved by its “sponsors,” KeyBank and Heartland Bank, that allowed anyone with a computer and a little technical savvy easy access to the Confidential Payment Card Data, (ii) and KeyBank and Heartland Bank, as Heartland’s “sponsors” and principals, failed, among other things, to properly monitor, audit, oversee and confirm that Heartland’s Payment Card processing system safeguards were adequate, complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained, and were fully operational.

**10.** Once Heartland’s Payment Card processing system was accessed by the data thieves, Heartland, which was quickly put on notice of its unauthorized visitors, and Defendants, which knew or should have known that Heartland’s security system had failed and allowed the

unwanted visitors to enter, did very little to determine what Heartland's guests were doing or how long they would stay. As it turns out, they stayed for over a year, and neither Heartland nor Defendants found them. During that time, Heartland's lack of Payment Card processing system security, its desire to use a "lowest bidder" system of selecting its outsourced IT "auditors," its reliance on a "snapshot" telling it that, at one identifiable point in time its system supposedly complied with the bare minimum industry standards, its startlingly poor IT oversight in general, and Defendants' complete and utter disregard of the oversight responsibilities they had to their fellow members of the Associations allowed the intruders to make trip after trip in and out of the Heartland Payment Card processing system.

11. The Confidential Payment Card Data compromised by the Data Breach included data taken from Payment Cards that Plaintiffs—as Issuers—issued to their customers. As a direct and/or proximate result of the Data Breach—and after being notified of the Data Breach by Visa and/or MasterCard, but not by Defendants or Heartland—Plaintiffs were compelled to cancel the compromised Payment Cards containing the Confidential Payment Card Data that Defendants and Heartland allowed to be taken, incur costs associated with the cancellation of the compromised Payment Cards, issue replacement Payment Cards to their customers, and incur other costs, expenses and losses. Given the magnitude of the Data Breach, Plaintiffs' expenses to cancel and reissue replacement Payment Cards and otherwise mitigate their losses are substantial and include, *inter alia*, costs for purchasing new plastic Payment Cards, postage and other mailing expenses, time spent by employees addressing the Data Breach, absorption of fraudulent charges made on the compromised Payment Cards, and harm to Plaintiffs' reputations and goodwill. Plaintiffs' damages are the imminently foreseeable result of Defendants' complete

and total abdication of their responsibility and duty to oversee the Heartland Payment Card processing system.

**12.** Immediately after Heartland's public disclosure of the Data Breach in January 2009, Robert H.B. Baldwin, Jr. ("Baldwin"), Heartland's President and Chief Financial Officer, was reported to say that "there are a host of things we didn't go into that we're implementing, some larger, some smaller..." and "[c]learly we need to do more [to secure this information]." Following at least two third-party forensic investigations of the Data Breach, Heartland was removed from Visa's list of approved payment processors because of, among other things, Heartland's non-compliance with the PCI-DSS data security standards, a failure that was proximately caused by Defendants' failure to comply with their oversight responsibilities.

**13.** As a direct result of the Data Breach, KeyBank was assessed substantial fines by both Visa and MasterCard because, among other things, it was the sponsor and principal of Heartland and because it failed to perform its oversight responsibilities and obligations. On information and belief, Heartland Bank also was fined for the same reasons.

**14.** Plaintiffs bring this class action on behalf of themselves and all similarly situated banks, credit unions and other financial intuitions that were injured by the Data Breach (as described above) as a direct and proximate result of Defendants' failure to, among other things, properly monitor, audit, oversee and confirm that Heartland's Payment Card processing system safeguards were adequate, complied with all applicable laws, contracts and guidance, were in place, were being properly monitored, managed, updated and maintained, and were fully operational which, in turn, directly and/or proximately resulted in the Data Breach. Plaintiffs specifically bring this action to recover, *inter alia*: (i) the out-of-pocket expenses associated with notifying their customers of the Data Breach, (ii) the out-of-pocket expenses to cancel the

Payment Cards compromised by the Data Breach and issue replacement Payment Cards, and (iii) all unauthorized charges made to the compromised Payment Cards that were (and continue to be) absorbed by Plaintiffs.

### **PARTIES**

**15.** Plaintiff Lone Star National Bank, N.A. (“Lone Star”) is a financial institution with its principal place of business in Pharr, Texas. Lone Star is a member of both Networks. Lone Star is both an Acquirer and an Issuer. Lone Star reissued Payment Cards compromised by the Data Breach, which caused Lone Star to suffer injuries.

**16.** Plaintiff PBC Credit Union (“PBC”) is a financial institution with its principal place of business in West Palm Beach, Florida. PBC is a member of both Networks. PBC is both an Acquirer and an Issuer. PBC reissued Payment Cards compromised by the Data Breach, which caused PBC to suffer injuries.

**17.** Plaintiff O Bee Credit Union (“O Bee”) is a financial institution with its principal place of business in Tumwater, Washington. O Bee is a member of both Networks. O Bee is an Issuer only. O Bee reissued Payment Cards compromised by the Data Breach, which caused O Bee to suffer injuries.

**18.** Plaintiff Seaboard Federal Credit Union (“Seaboard”) is a financial institution with its principal place of business in Bucksport, Maine. Seaboard is a member of both Networks. Seaboard is an Issuer only. Seaboard reissued Payment Cards compromised by the Data Breach, which caused Seaboard to suffer injuries.

**19.** Plaintiff Pennsylvania State Employees Credit Union (“PSECU”) is a financial institution with its principal place of business in Harrisburg, Pennsylvania. PSECU is a member

of both Networks. PSECU is both an Acquirer and an Issuer. PSECU reissued Payment Cards compromised by the Data Breach, which caused PSECU to suffer injuries.

**20.** Defendant KeyBank is an Ohio corporation with its principal place of business at 127 Public Square, Cleveland, Ohio 44114. KeyBank is a wholly-owned subsidiary of KeyCorp, a bank and financial holding company that is publicly traded on the New York Stock Exchange (symbol: KEY). KeyBank is one of the nation's largest banks with over ninety-seven billion dollars (\$97,000,000,000 USD) of assets as of September 30, 2009. KeyBank provides a wide range of retail and commercial banking, commercial leasing, investment management, consumer finance, Payment Card and investment banking products and services to individuals, merchants, small businesses and large corporate and institutional clients through its over 1000 branches and offices located in fourteen (14) states. KeyBank is a member of both the Visa and MasterCard Networks. On information and belief, KeyBank is both an Acquirer and an Issuer. KeyBank is authorized to conduct business in the State of Texas.

**21.** Defendant Heartland Bank is a Missouri corporation with its principal place of business at 7818 Bonhomme, Clayton, Missouri 63105. Founded in 1887, Heartland Bank is a full-service, independent bank with assets totaling more than \$1 billion. Heartland offers products and services for personal banking, including Payment Cards, business banking, home mortgage loans and commercial lending services. Heartland Bank is a member of both the Visa and MasterCard Networks. On information and belief, Heartland Bank is both an Acquirer and an Issuer.

#### **JURISDICTION AND VENUE**

**22.** This Court has subject matter jurisdiction over this class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in

controversy exceeds five million dollars (\$5,000,000), exclusive of interest and costs, and some members of the proposed Classes are citizens of states different than Ohio and/or Missouri. 28 U.S.C. § 1332(d)(2)(A). This Court also has subject matter jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367.

23. Part of the events and/or omissions giving rise to the Plaintiffs' claims have occurred and/or originated in the Southern District of Texas. Closely related litigation, MDL No. 2046, *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation* (Rosenthal, J.), was transferred to the Southern District of Texas for coordinated pre-trial proceedings by the Judicial Panel on Multidistrict Litigation. Venue, therefore, is proper in the Southern District of Texas pursuant to, *inter alia*, 28 U.S.C. § 1391(a).

### **FACTUAL BACKGROUND**

#### **A. Overview of the Visa and MasterCard Associations and the United States Payment Card Industry.**

24. This case involves Visa and MasterCard, two (2) of the four (4) major systems, or Networks, that provide authorization and settlement services for United States Payment Card transactions, the two other systems being American Express and Discover. Visa and MasterCard Association member financial institutions (*e.g.*, Plaintiffs and Defendants) issue Payment Cards with the Visa and MasterCard brands. A credit card permits a cardholder to pay only a portion of the balance due on the account. A consumer's use of a debit card, on the other hand, allows a merchant to immediately access money directly from a cardholder's checking or deposit account. Because Visa and MasterCard Payment Cards are accepted at numerous, unrelated merchants, they are known as general purpose cards (as opposed to proprietary cards, such as those issued by department stores like Sears or Macy's, which are accepted only at those stores).

**25.** Visa and MasterCard are structured as open, joint venture associations (*i.e.*, the Associations). Members of the Associations (*i.e.*, financial institutions) that issue Payment Cards are known as “Issuers.” Members of the Associations that acquire merchants and/or merchant transactions for the Networks are known as “Acquirers.” Some members of the Associations serve as both Issuers and Acquirers.

**26.** The Associations, in fact, are legal “associations” of members. By agreement and by conduct, each Association (Visa and MasterCard) constitutes an enterprise undertaken by their member financial institutions for the mutual benefit of all the members, an enterprise in which the members combine their property, money, skills and knowledge in a community of interest and with a common purpose. The members have a close and special relationship with one another, are closely linked and are intertwined through their membership in the Associations and use of the Networks.

**27.** Visa and MasterCard are publicly traded corporations, but nevertheless have members and membership interests; both are operated, as is relevant here, as associations with each “member” being a part of either or both Associations. Any financial institution eligible for Federal Deposit Insurance Corporation (“FDIC”) insurance is eligible for membership in the Associations.

**28.** Visa Association members have the right to issue Visa Payment Cards and/or acquire Visa Payment Card transactions from merchants that accept Visa Payment Cards. In exchange, the Visa Association members must follow Visa's by-laws and operating regulations. The same is true of MasterCard Association members.

**29.** Visa has approximately 14,000 financial institution Association members in the United States. MasterCard has approximately 20,000 global financial institution Association

members. At least 20 million merchants accept Visa and/or MasterCard Payment Cards. Whatever the exact membership number may be at any given time, each Association is a finite, easily identifiable group of financial institutions. At all relevant times, Defendants had actual knowledge that any financial institution that is an Issuer and/or an Acquirer of Visa and/or MasterCard branded Payment Cards was a member of one or both Associations.

**30.** The processing of a consumer Payment Card transaction is complex and involves numerous independent business entities, including merchants, Acquirers, Issuers, authorizing processors, third party processors, independent sales organizations, the Associations, ACH processors, the government and other entities.

**31.** The purchase of goods or services with a Payment Card triggers two sequences of events—with data security the foundation and core of each sequence. First, when a consumer uses a Payment Card to purchase goods and/or services at a merchant, the approval or “*authorization*” process commences. Second, if authorization is secured, the “*settlement*” process is triggered, whereby all parties involved in the transaction are paid by the consumer.

**32.** The “*authorization*” process generally involves the following steps, all of which are collectively referred to as a data “loop:”

- (i) A consumer uses a Payment Card to pay a merchant for goods or services. The sales data is entered into the merchant’s point of sale (POS) system, the Payment Card is “swiped” on the POS device and the data on the Payment Card’s magnetic strip is “read” by the POS device.
- (ii) The amount of the transaction and the data embedded in the Payment Card is electronically transmitted by the merchant to an Acquirer Payment Card processor, which can be the Acquirer itself, a non-financial institution or a series of entities that have contracted, directly or indirectly, with the merchant and/or the Acquirer to provide Payment Card transaction authorization services.
- (iii) The Acquirer Payment Card processor sorts the data (Visa or MasterCard) and transmits the information into either the Visa or MasterCard Network, whichever is applicable.

- (iv) The Visa/MasterCard Network sorts the data and routes it to an Issuer Payment Card processor, which can be the Issuer itself or a series of entities that have contracted, directly or indirectly, with the Issuer to provide Payment Card transaction authorization services.
- (v) The Issuer Payment Card processor, or the Issuer itself, examines the data, validates the Payment Card and determines whether there are funds or credit available to pay for whatever the consumer is attempting to purchase. Based on this analysis, the Issuer Payment Card processor either authorizes or declines the transaction.
- (vi) The Issuer Payment Card processor, or the Issuer itself, “loops” the authorization/declination back to the merchant—all within a few seconds of the original “swiping” of the Payment Card on the merchant’s POS device. If authorized, the consumer signs the POS device or the sales receipt for the transaction and the sales information is “captured” by the merchant. If declined, the consumer is so advised.

See also the Anatomy of a Visa Transaction and the Anatomy of a MasterCard Transaction attached as **Exhibits “A”** and **“B,”** respectively.

**33.** At the end of the day, the merchant combines all of its “captured” sales for the day into a “batch” and the processing moves into the second stage—“*settlement.*” The settlement process, another “loop,” generally occurs as follows:

- (i) The merchant sends a batch of transactions to its Acquirer Payment Card processor requesting payment.
- (ii) The Acquirer Payment Card processor sorts the transactions by Payment Card type—Visa or MasterCard—and routes the “batch” into the Visa or MasterCard Network, typically via the same entities that were involved during the authorization loop.
- (iii) Once in the Visa/MasterCard Network, Visa/MasterCard sorts the “batch” and routes the transaction data to the consumers’ Issuer financial institutions.
- (iv) Ultimately, the Issuers, after validating their earlier authorizations, take the necessary funds from the cardholders’ accounts (or adds the charge to the cardholders’ credit accounts) and forward payment back through the Network. Along the way, each entity takes a “fee” as the funds travel back to the merchant. Since actual “cash” is involved, FDIC regulated financial institutions (*i.e.*, the

Acquirers) must be involved. The Acquirers deposit the net funds, after all fees have been deducted, into the merchant's bank account.

**34.** In a Visa or MasterCard Payment Card purchase, the merchant actually receives approximately 98% of the price of the good or service sold. The remaining 2%, known as the "merchant discount," is the fee paid to the merchant's Acquirer bank for providing the Payment Card processing services. The Acquirer, in turn, splits the fee with the Payment Card Issuer, which receives approximately 1.4 % of the purchase price. The Issuer receives the majority of the fee because it owns the consumer's account and assumes the risk of non-payment. The 1.4 % of the fee paid to the Issuer is called the "interchange fee."

**35.** The Visa and MasterCard Associations are supported primarily by service and transaction fees paid by their members (such as Plaintiffs and Defendants). Visa and MasterCard set their fees to cover the costs involved in providing the basic infrastructure to the members, but do not charge license fees or royalties to their members.

**36.** The finite, identifiable groups of Visa and MasterCard Association members work together through each of the Associations to achieve special benefits for themselves that they could not provide independently, including access to globally recognized brands and sophisticated computer networks for processing transactions.

**37.** Today, Visa and MasterCard Payment Cards are issued by thousands of Association members (such as Plaintiffs and Defendants) and may be used nationally and internationally at millions of merchants, all of which works to the common benefit of the members of the Associations. Minimum financial qualifications required for a Payment Card have declined dramatically so that even consumers with lower incomes are readily able to obtain them. The percentage of households with Payment Cards quadrupled from 16% in 1970 to 68%

in 1998. The share of consumer spending paid for with general purpose Payment Cards has increased from less than 3% in 1975 to 18.5 % in 1999.

**38.** As a result, consumers have access to products that combine the many features available through the Visa and MasterCard Associations with features and services developed by the individual Issuers. Cardholders today can choose from thousands of different card products with varying terms and features, including a wide variety of rewards and co-branding programs and services such as automobile insurance, travel and reservation services, emergency medical services and purchase security/extended protections programs. The members of the Associations reap the benefits of their joint venture and association with one another through the fees they earn by processing billions of dollars in transactions through the Networks. The security of the Confidential Payment Card Data is essential to consumers and members of the Association alike.

**B. The Visa/MasterCard Associations and their Members and Nonmembers.**

**39.** The Associations themselves do not issue Payment Cards, but rather, provide a clearinghouse system for charges and payments on the Payment Cards and license financial institutions to use the Visa and MasterCard brand names. The Associations set and enforce rules, regulations and operational and interchange procedures governing their branded Payment Cards. Members of the Associations are financial institutions licensed or otherwise authorized by the Associations to issue the branded Payment Cards (Issuers), contract with the merchants to accept the Payment Card transactions (Acquirers), or both.

**40.** Issuers are responsible for their Payment Card programs, which encompass nearly all aspects of cardholder account activity, including: marketing to new potential cardholders; processing cardholder applications; establishing credit limits and policies; overseeing design, manufacturing and embossing of Payment Cards; issuing and reissuing Payment Cards;

overseeing PIN numbers; maintaining authorization files; providing customer service; processing payments and handling settlements through the interchange; and establishing collection operations. Because Issuers (such as Plaintiffs) have no control over the majority of the interchange system, they must depend and rely on the Acquirers (such as Defendants) to properly and adequately carry out their risk management and fraud detection/prevention duties—in this case, the work of properly, diligently and adequately monitoring, auditing, overseeing and confirming that, at the relevant times, Heartland's Payment Card processing system safeguards were adequate, complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained, and were fully operational in order to protect confidential Payment Card data that was being processed.

**41.** Acquirers contract with merchants to (i) accept merchant sales drafts, (ii) provide authorization terminals, instructions and support, and (iii) handle the processing of Payment Card transactions. In short, Acquirers establish and manage the merchants' accounts. An Acquirer's key responsibilities include (i) recruiting and setting up new merchants with merchant accounts, (ii) investigating procedures on disputed transactions, (iii) pricing of discount rates and fees to the merchants, (iv) establishing merchant acceptance guidelines, (v) providing support services for merchants (customer service, voice authorizations, etc), (vi) managing risk and engaging in fraud prevention and detection, and (vii) monitoring and auditing data security procedures and controls of the third party nonmembers with which it enters into contracts pertaining to Payment Cards.

**42.** Each Acquirer is a member of the Visa or MasterCard Association and agrees to follow the Association rules and regulations. Some financial institutions are both Issuers and Acquirers (*e.g.*, Defendants and all Plaintiffs other than O Bee and Seaboard). Visa and

MasterCard require merchants in their respective Associations to be financially responsible and of good reputation. Each merchant has a written contract with its Acquirer to accept the Visa or MasterCard Payment Card in payment for transactions and abide by the terms of the contract. An Acquirer generally owns the BIN (“Bank Identification Number”) and provides back room operations. It also carries the risk of charge-backs, which can be significant if a merchant is unable or unwilling to honor its financial liability. The FDIC Credit Card Activities Manual, *Merchant Processing* (“FDIC Guidance”) observes in the section, “*Risks Associated with Merchant Processing*,” that Acquirers that do not devote sufficient resources to oversight or perform proper due diligence reviews of prospective third-party processors take a risk, and many of an Acquirer's risks are interdependent with Payment Card system operators and third parties. The FDIC Guidance further states that Acquirers also have compliance risks that arise not only from the failure to follow Association rules and regulations, but also from clearing and settlement rules, suspicious activity reporting requirements and a myriad of other laws, regulations and guidance.

**43.** As such, the applicable standard of care requires Acquirers to, among other things, (i) have a structured compliance management program in place, (ii) ensure the internal control environment is sound, and (iii) confirm that staff is knowledgeable. In the section, *Third-Party Relationships*, the FDIC Guidance charges Acquirers with (i) maintaining suitable controls over each and every third party relationship the Acquirer might enter into to further the Acquirer's contractual obligations, (ii) employing proper due diligence to identify and select third party entities with which to contract, (iii) maintaining comprehensive, written contracts between the Acquirer and third parties, and (iv) employing ongoing oversight of third parties and

their activities, including determining whether any changes to the relationships are warranted and/or whether the relationship should be discontinued.

**44.** There are several types of third parties involved with Visa/MasterCard Association members in connection with Payment Card processing. For example, Third Party Processors contract with Acquirers to authorize, capture, settle and clear transactions. Some Third Party Processors also perform back office or service functions for the Acquirers, such as maintaining a 24-hour customer service help desk, chargeback and retrieval request processing, issuing statements, risk management and/or credit underwriting.

**45.** Another type of third party entity involved with the Visa/MasterCard Association members is an Independent Sales Organization (“ISO”). An ISO is an entity registered with Visa to provide merchants with the ability to accept Visa Payment Cards. An ISO must be sponsored by an Acquirer that is a member of the Visa Association and pays annual registration fees to Visa. The MasterCard equivalent of a Visa ISO is known as a Member Service Provider (“MSP”). Neither an ISO nor a MSP can have access to the Visa or MasterCard Associations without first having an FDIC regulated Association member “sponsor” it into the association. As a result, the other members of the Association through which Payment Card data passes must, by the nature of the Payment Card system, rely exclusively on the “sponsor” of the ISO/MSP to properly, diligently and adequately monitor, audit, oversee and confirm that the “sponsor’s” ISO/MSP’s Payment Card processing system safeguards are always adequate, always comply with all applicable laws and guidance, are always in place, are always being properly monitored, managed, updated and maintained, and are always fully operational in order to protect the Confidential Payment Card Data transmitted through the Networks.

46. Since any financial institution eligible for FDIC insurance is eligible for Visa and/or MasterCard Association membership, the FDIC has supervisory control over the Associations and their members.

47. The FDIC has determined that Payment Card issuance and merchant acquisition are banking activities with banking risks. As such, the FDIC has established definitions, regulations and examination procedures delineating the interdependent relationships by and between the Association members, including the duties owed by the Issuers and Acquirers to each other. For example, the FDIC Guidance, *Merchant Processing*, notes that the failure of any payment system participant to provide funding for settlement may precipitate liquidity or credit problems for other participants. This is an important acknowledgment of the interdependence of and special relationship between all parties participating in the Visa/MasterCard Associations—including Plaintiffs and Defendants—and it establishes the foreseeability that a failure by one member of an Association in its obligations may cause harm to one or more other members of the finite and identifiable group of entities that are also part of the same Association.

**C. Duties of the Acquirers in the Visa/MasterCard Associations.**

48. In the Association structures, the Acquirers assume the basic Payment Card transaction risks, including processing the transaction properly and providing adequate controls on the transaction. As part of this function, the FDIC notes that risk occurs from employee error, misconduct, a breakdown of computer systems and/or natural catastrophes. The FDIC states that to be a merchant Payment Card processor, an Acquirer must have adequate and knowledgeable staff, a sound internal control environment, appropriate technology, comprehensive operating procedures and effective contingency plans.

**49.** The FDIC Guidance clearly states that the Visa/MasterCard Association by-laws and operating rules and regulations make their members fully responsible for the actions of any and all third party entities with which they contract. The FDIC Guidance, *Third Party Relationships*, emphasizes that Acquirers remain responsible to ensure that Payment Card activities are conducted in a safe and sound manner when employing third party entities of any type to perform processing functions. This accountability may not be contracted away:

Whether in a franchising or outsourcing fashion, a bank's use of third parties for credit card program functions does not diminish management's responsibility to ensure that the activities are conducted in a safe and sound manner as well as in compliance with applicable laws and guidance. An absence of adequate policies for managing third-party arrangements, including selection and oversight, is normally cause for concern. Examiners should also normally expect to see that management subjects third-party relationships to the same risk-management, security, privacy, and other consumer-protection policies as if the bank conducted the activities directly.

Credit Card Activities Manual. Chapter XX ([www.fdic.gov/regulations/examination](http://www.fdic.gov/regulations/examination)).

**50.** In addition to the FDIC rules, handbooks promulgated by the Federal Financial Institutions Examination Council (FFIEC) contain numerous recommendations setting forth additional applicable standards of care and duties of financial institutions when contracting with third party entities to perform work within the Associations. These FFIEC Handbooks reiterate much of the same guidance and many of the same standards promulgated by the FDIC:

- Although merchant acquiring financial institutions [*i.e.*, Acquirers] may use third parties to perform many acquiring activities, the acquiring financial institution is responsible for all third-party processor and merchant activity. FFIEC Retail Payment Systems IT Examination Handbook (March 2004) at 15.
- Financial institutions engaged in retail payment systems should establish an appropriate risk management process that identifies, measures and limits risks. *Id.* at 24.
- Financial institutions should establish internal risk management systems that are commensurate with the size and complexity of their operations. *Id.* at 25.

- Because financial institutions often rely on third-party service providers for retail payment system products and services, the strategic plan should include a comprehensive vendor management program. *Id.* at 26.
- Financial institutions are responsible for risks associated with the activities of third-party service providers with which they contract. *Id.* at 27.
- Operational risk can also arise from fraud . . . . Operational risk controls should include information system, procedural, administrative, and legal measures to prevent . . . financial loss as a result of operational risk. System measures include . . . encryption techniques to ensure . . . transaction information integrity. *Id.* at 30-31.
- Due to the potential large retail transaction volumes and associated dollar values when initiating payments, internal audit coverage is critical for effective oversight of the financial institution's retail payment systems. The board of directors should ensure an information technology audit program is in place and designed to test retail payment system internal controls and management policies and procedures. *Id.* at 31.
- Financial institutions must implement the appropriate physical and logical security controls to ensure retail payment system transactions are processed, cleared and settled in a . . . reliable manner. Retail payment systems contain confidential customer information subject to GLBA section 501(b) security guidelines. The board and management are responsible for protecting the confidentiality, integrity and availability of these systems and data. The privacy risk . . . should cause these systems to rank high in all institutions' information security risk assessments. . . . An institution's risk assessment should require it to protect retail payment systems from unauthorized access through appropriate network configuration, firewalls or intrusion detection. *The assessment should review the security of all third-party service providers as well. Id.* at 33 (emphasis added).
- Financial institutions *must* establish and maintain effective vendor and third-party management programs. . . . To ensure retail payment operations are conducted appropriately, financial institutions should have appropriate contract provisions and adequate due diligence processes. They should also monitor service providers for compliance. . . . The financial institution must also maintain effective control over service provider access to customer and financial institution information consistent with GLBA 501(b). Contractual provisions should define the terms of acceptable access . . . . *Id.* at 35-36 (emphasis added).
- Financial institutions should adopt measures that limit operational risks for the processing, clearing and settlement of retail payments . . . . Risk analysis should identify confidential assets, critical operations, and potential threats. It should

also define safeguards and countermeasures to provide adequate protection. *Id.* 36.

**51.** At least three other FFIEC Handbooks outline and discuss the various types of controls that the standard of care requires financial institutions—such as Defendants—to utilize to ensure that security is adequate at its processors, ISOs, MSPs, and other third party entities with which it contracts—such as Heartland. *See, e.g.*, FFIEC Outsourcing Technology Services Handbook (June 2004); FFIEC Supervision of Technology Service Providers Handbook (March 2003); and FFIEC Information Security Handbook (July 2006). For example, the FFIEC Information Security Handbook states, among other things, that:

- Financial institutions should implement an ongoing security process and institute appropriate governance for the security function. . . . The process includes five areas . . . Information Security Risk Assessment . . . Information Security Strategy . . . Security Controls Implementation . . . Security Monitoring . . . (and) Security Process Monitoring and Updating. *Id.* at 4.
- Financial institutions must maintain an ongoing information security risk assessment program that effectively gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements . . . . *Id.* at 9.
- The evaluation of controls should also encompass the risks to information held and processed by service providers . . . . *Id.* at 14.
- Financial institutions should secure access to their computer networks through multiple layers of access controls to protect against unauthorized access. *Id.* at 37.
- Financial institutions should employ encryption to mitigate the risk of disclosure . . . of sensitive information . . . in transit. *Id.* at 56.
- Financial institutions should protect against the risk of malicious code by implementing appropriate controls at the host and network level to prevent and detect malicious code . . . . Typical controls to protect against malicious code use technology, policies and procedures, and training, all applied in a layered manner *from perimeters inward* to hosts and data. . . . Controls are applied at the host, network and user levels. *Id.* at 60-61 (emphasis added).

- When deploying off the shelf software, management should harden the resulting system. *Id.* at 67.
- Financial institutions should exercise their security responsibilities for outsourced operations through . . . independent review of the service provider’s security through appropriate audits and tests. . . . Financial institutions are required under the 501(b) guidelines to ensure service providers have implemented adequate security controls to safeguard customer information. The guidelines require institutions to . . . monitor service providers to confirm that they are maintaining those controls when indicated by the institution’s risk assessment. . . . Financial institutions should obtain access to the TSP for institution or independent third party evaluations of the TSP’s performance against the standard. (SAS 70 audits can be used in “lower risk relationships.”) *Id.* at 76-77.
- Financial institutions should carefully and critically evaluate whether a SAS 70 report adequately supports their oversight responsibilities. The report may not . . . address the effectiveness of the security process in continually mitigating changing risks. . . . (It) may not address whether the TSP is meeting the institution’s specific risk mitigation requirements. Therefore, the contracting oversight exercised by financial institutions may require additional tests, evaluations and reports to appropriately oversee the security program of the service provider. *Id.* at 77-78.
- Management . . . evaluating TSPs should use the guidance in this booklet in . . . exercising ongoing oversight or audit responsibilities. *Id.* at 93.
- Financial institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of existing security controls. They should then use that information to update the risk assessment, strategy, and implemented controls. A static security system program provides a false sense of security and will become increasingly ineffective over time. Monitoring and updating the security program is an important part of the ongoing cyclical security process. *Id.*, pg. 95.

**D. Overview of the Relationships between the Visa/MasterCard Association Members.**

**52.** All Visa/MasterCard Association members (such as Plaintiffs and Defendants) agree to follow each Association’s by-laws and operating regulations and, as a result, are contractually bound to each other.

**53.** Association members also individually contract with persons and entities outside the Association structure – *i.e.*, merchants, cardholders and third party service providers (such as

Heartland). The contracts between Association members and nonmembers bind the nonmembers to each Association's by-laws and operating regulations. On the other hand, formal contracts are not necessary between Association members because they are contractually bound to each other through the Visa/MasterCard Association by-laws and operating regulations and through the implied contracts, agreements and duties that arise from the members' special relationships to one another.

**54.** All Association members are third party beneficiaries of each other member's contracts with nonmember, third party entities, regardless of whether they are signatories because, *inter alia*: (i) the Association members have a "close relationship" with each other through the Networks, (ii) the non-signatory Association members are "closely linked" to the signatory member's cardholders, and (iii) the cardholders are "intertwined" with their Issuer and all other Issuers.

**E. The Relationships between Defendants and Heartland.**

**55.** Heartland describes itself as "one of the nation's largest payment processors delivering credit/debit/prepaid card processing, payroll, check management and payments solutions." Since being founded in 1997, Heartland has grown to service 175,000 merchants at 250,000 business locations nationwide, with 2008 revenue of \$1.54 billion.

**56.** According to Heartland's 2008 Form 10-K filed with the SEC on March 19, 2009, the Payment Card processing services it performs include "facilitating the exchange of information and funds between merchants and cardholders' financial institutions, providing end-to-end electronic payment processing services to merchants, including merchant set-up and training, transaction authorization and electronic draft capture, clearing and settlement, merchant accounting, merchant assistance and support and risk management." Heartland derives its

compensation from a combination of a percentage of the merchants' gross processing fees and a flat fee per transaction. For example, for every \$100 purchase processed through Heartland's Payment Card processing system, Heartland receives approximately 52 cents of revenue.

**57.** In connection with its Payment Card transaction processing business as a "sponsored" ISO/MSP and agent of Defendants, Heartland received and was entrusted with the Confidential Payment Card Data of millions of customers whose Payment Cards were issued by Plaintiffs and compromised by the Data Breach.

**58.** Also according to Heartland's 2008 Form 10-K, "substantially all" of Heartland's revenue is derived from processing and settling Visa and MasterCard Payment Card transactions for Defendants' merchant customers.

**59.** Pursuant to the Merchant Processing Agreements (MPAs) between Defendants and Heartland, at all relevant times, KeyBank and Heartland and Heartland Bank and Heartland were (and continue to be) in contractual relationships.

**60.** Pursuant to the MPAs and the Visa and MasterCard rules, regulations and definitions, Heartland, as a third party, an ISO and an MSP, was (and continues to be) Defendants' agent and, at all relevant times, acted within the course and scope of that agency when it was in possession of the Confidential Payment Card Data of the customers whose Payment Cards were issued by Plaintiffs and compromised by the Data Breach.

**61.** Pursuant to its June 30, 2009 Form 10-Q, KeyBank states that "[u]nder an agreement between KeyBank and Heartland [*i.e.*, the MPA], Heartland utilizes KeyBank's membership in the Visa and MasterCard networks to register as an Independent Sales Organization (ISO) for Visa and a Member Service Provider (MSP) with MasterCard to provide merchant payment processing services for Visa and MasterCard transactions." KeyBank further

states that it “received letters from both Visa and MasterCard assessing fines, penalties or assessments relating to the [Heartland Data Breach]. KeyBank is in the process of pursuing appeals of such fines, penalties or assessments.” *Id.* Moreover, in the event Heartland “is unable to indemnify KeyBank for these charges, KeyBank acknowledges that its ultimate liability related to the intrusion “could be significant.” *Id.* On information and belief, the same is true for Heartland Bank.

**62.** Heartland’s June 30, 2009 Form 10-Q states that its business model is to provide “payment processing services related to bank card transactions for merchants” and that the company’s revenues are primarily derived from “processing and settling Visa and MasterCard bank card transactions for its merchant customers.” The Heartland Form 10-Q further acknowledges that it cannot be a “member” of the Visa or MasterCard Associations, so it “has entered into sponsorship agreements with member banks [*i.e.*, the Defendants].” *Id.* These “sponsorship agreements” permit “the company to route Visa and MasterCard transactions under the member bank’s control and identification numbers to clear credit bank card transactions through Visa and MasterCard.” *Id.* The sponsorship agreements also “enable the company to settle funds between cardholders and merchants by delivering funds to the member bank, which in turn transfers settlement funds to the merchants’ bank accounts.” *Id.*

**63.** Thus, at all relevant times, within the Visa/MasterCard Network context, Heartland was (and continues to be) an ISO/MSP/Acquirer, a Third Party Processor (both authorization and payment) and an agent of its sponsors and principals including, most prominently, KeyBank—through which 67% of its Third Party Processor business flows.

**F. The Heartland Data Breach.**

**64.** In December, 2007, an SQL (“Structured Query Language”) injection occurred in the Heartland Payment Card Processing system in a merchant facing payroll page. Heartland claims it found the injection and believed that, according to CEO Carr, it “cleaned it up” very quickly. Defendants failed to properly, diligently and adequately monitor, audit, oversee and confirm that Heartland, its “sponsored” agent, did, in fact, “clean it up,” however, and likewise failed to take all reasonable and necessary steps to ensure that the deficiencies in the system that allowed the SQL injection to occur in the first place were modified or fixed and/or confirm that any revisions that were made would, from that point forward, be adequate and comply with all applicable laws and guidance, remain in place, be properly monitored, managed, updated and maintained and always be fully operational in order to protect the Confidential Payment Card Data transmitted through the system. Thirteen (13) months later, the “clean up” efforts would be seen for what they were—worthless.

**65.** Defendants fostered an unsecure Payment Card processing system environment at Heartland, through their complete lack of compliance with their ongoing security oversight obligations (as more fully set forth above) that, in turn, allowed the SQL injection to occur, failed to “clean it up” and failed to ensure that their agent, Heartland, sufficiently “cleaned it up.”

**66.** Because Defendants failed to comply with their obligations, duties and responsibilities (as more fully set forth above), Defendants allowed and permitted the SQL injection, which Heartland supposedly “cleaned up,” to go far beyond a “merchant facing payroll page.” Defendants’ failures resulted in the loss of Confidential Payment Card Data from millions of Payment Cards issued by Plaintiffs and similarly situated financial institutions.

**67.** Just a few months later, in March, 2008, Heartland learned about the theft of Confidential Payment Card Data from Hannaford Brothers, a retail grocery chain in the Northeast. Defendants knew or should have known about this attack as well since it was highly publicized and Defendant KeyBank had, for many years, utilized the premises of Hannaford Brothers stores to house its full service banking facilities. In fact, long before the Data Breach in January 2007, a major data breach within the TJX Companies (also committed by the same hackers who committed the Data Breach using the same or similar methods used in the Data Breach) was front-page news in general-interest magazines and newspapers throughout the country. As widely publicized as the TJX data breach was in the popular media, it was even more prominently publicized within the narrow Payment Card security community. Despite knowing about the TJX data breach and the Hannaford Brothers data breach, Defendants failed to take all reasonable and necessary steps to ensure that the deficiencies in the Hannaford Brothers and TJX computer systems did not exist at Heartland. In fact, at least according to Heartland, Defendants did nothing.

**68.** In accordance with their rules, regulations and operating procedures, both Visa and MasterCard monitor their respective Associations for potential fraudulent activity. When suspected fraudulent use of Payment Cards is identified, MasterCard notifies the affected Issuers through a Security Alert. Similarly, Visa notifies the affected Issuers through an alert known as a “Compromised Account Management Systems Alert,” or “CAMS Alert.” Upon information and belief, these alerts generally set forth the type of compromised data, the relevant timeframe of the compromise and a list of the compromised Payment Card numbers.

**69.** In October 2008, Visa reportedly advised Heartland—via a CAMS Alert—about “suspicious activity surrounding certain cardholder accounts.” Heartland’s IT team subsequently

worked with forensic auditors from the major card brands (*i.e.*, Visa, MasterCard, American Express and Discover) to locate the entry point and identify the nature and extent of the Data Breach. Again, Defendants did nothing to comply with their oversight responsibilities and obligations to ensure that the steps taken by Heartland were sufficient and adequate to find the intrusion and deal with it effectively.

**70.** Heartland eventually retained a forensic IT company that, according to Heartland CEO Carr, found “some data files that looked strange.” No one from Heartland or Defendants previously had discovered these “strange” data files. Once discovered, however, it took Heartland—as Carr admitted—only a “few hours” to find the malicious software that created the “strange” files.

**71.** Heartland first publicly disclosed the breach on January 20, 2009 amid the hoopla and fanfare of President Obama’s inauguration.

**72.** In its SEC filings, Heartland claims that the Data Breach “involved malicious software [“malware”] that appears to have been used to collect in-transit, unencrypted payment card data while it was being processed by Heartland during the transaction authorization process.” Malware is malicious software that can be programmed to, *inter alia*, identify, store and export information (including Payment Card information) from compromised computer systems.

**73.** In one of his many interviews after the Data Breach, Heartland CEO Carr described the malware as “[s]niffers [that] were put on the network by bad guys.” A sniffer is computer hardware and/or software that can intercept, capture and log traffic passing over a network. The sniffer involved in the Data Breach reportedly targeted Heartland’s “authorization

switch,” which sends unencrypted account data from merchants to the Issuers through the Visa/MasterCard networks.

74. In one of his many interviews after the Data Breach, Heartland President Baldwin further explained that the Data Breach had two parts. The first part consisted of key-logging malware, which penetrated Heartland’s firewall (*i.e.*, the system’s security barrier software). Key-logging malware can covertly capture anything typed on an infected computer, such as user names and passwords. A sniffer is similar to key-logging malware, but rather than merely capturing keystrokes, a sniffer can capture entire packets of data on a system.

75. According to Baldwin, in the second part of the Data Breach, the key-logging malware “was able to propagate a sniffer onto some of the machines in our network. And those are what were actually grabbing the transactions as they floated over our network.” Baldwin said that the malicious sniffer program “was watching the transactions as they moved on to our authorization switch, not in the switch itself.”

76. Heartland later acknowledged in its SEC filings that the information compromised in the Data Breach “included card numbers, expiration dates, and certain other information from the magnetic strip on the back of the payment card (including, for a small percentage of transactions, the cardholder’s name).” The Data Breach compromised approximately 130 million Payment Cards, most of which were replaced by Plaintiffs and similarly situated financial institution Issuers at substantial expense.

**G. After Heartland Revealed the Data Breach, KeyBank was Fined and Visa Removed Heartland from the List of PCI-DSS Compliant Companies.**

77. The Payment Card Industry Data Security Standards (commonly referred to as “PCI DSS”) is a set of minimum requirements for enhancing Confidential Payment Card Data security designed to reduce the likelihood of a data breach occurring. According to a statement

released by Visa pertaining to the Data Breach, “[c]ompliance with the PCI DSS has significantly reduced unauthorized access to cardholder data.”

**78.** The PCI-DSS standards are issued by an organization called the Payment Card Industry Security Standards Council (the “PCI Security Standards Council”). The PCI-DSS are essentially a checklist of measures for Payment Card processors and merchants, and include requirements for, among other things, security management, policies, procedures, network architecture, software design and other critical protective measures.

**79.** In order to be PCI-DSS compliant, an applicant must be periodically audited and approved by a third party security vendor. These independent “assessment” entities, which Defendants allowed Heartland to select using a “lowest bid” method, are known in the industry as Quality Security Assessors, or QSAs. Assuming a QSA is adequately qualified and not restricted or impaired in performing its audit function by the entity being audited, a QSA’s determination that an entity is PCI-DSS compliant is nothing more than a finding that at the “snapshot” in time the audit was performed, the audited company allegedly met the standards.

**80.** Prior to the Data Breach, Heartland executives were well aware—and Defendants knew or should have been aware—that the bare minimum PCI-DSS standards were insufficient to protect it from an attack by sophisticated hackers. For example, on a November 4, 2008 Earnings Call with analysts, Carr remarked that “[w]e also recognize the need to move beyond *the lowest common denominator of data security, currently the PCI-DSS standards*. We believe it is imperative to move to a higher standard for processing secure transactions, one which we have the ability to implement without waiting for the payments infrastructure to change.” (emphasis added).

**81.** After the Data Breach, Visa investigated Heartland's security measures, after which Visa concluded that Heartland was not PCI-DSS compliant at the time of the initial security lapse. In fact, shortly after Heartland announced the Data Breach in January 2009 and Visa completed its forensic investigation, Visa removed Heartland from its list of PCI-DSS compliant processors and levied fines against its principal and "sponsor," KeyBank, and presumably Heartland Bank as well, for allowing their agent to operate while it was not PCI-DSS compliant. In discussing this very issue after the Data Breach, Visa's Chief Enterprise Risk Officer, Ellen Richey, stated:

I'm sure everyone in this room has read the headlines questioning how an event of this magnitude could still happen today. The fact is: *it never should have.*

As we've all read, the company had validated PCI compliance. *But it was the lack of ongoing vigilance in maintaining compliance that left the company vulnerable to attack. . . . As we've said before, no compromised entity has yet been found to be compliance with PCI DSS at the time of a breach.* <http://www.corporate.visa.com/media/ellen-richey-summit-remarks.pdf>. (emphasis added).

Ms. Richey went on to state that "cost-cutting" to "shortchange security measures" is both "short-sighted and dangerous." *Id.* Yet Defendants did exactly that, which allowed Heartland's Payment Card processing system "security" to fail.

**82.** In addition to removing Heartland from its PCI-DSS compliance list, Visa reportedly put Heartland on probationary status. Under the terms of the probation, Visa reportedly subjected Heartland to more-stringent security assessments, monitoring and reporting.

**83.** On a May 7, 2009 Earnings Call with Analysts, Carr revealed that MasterCard also had fined Heartland's "sponsor banks [including KeyBank] ostensibly because of an alleged failure by Heartland to take appropriate action upon having learned that its computer system may have been breached and upon thereafter having discovered the intrusion." On information and

belief, KeyBank was the only one of the Heartland sponsoring banks to be fined. The MasterCard fine reportedly was in excess of \$6 million.

**84.** On December 17, 2009, Heartland announced that it reached a settlement with American Express, pursuant to which Heartland agreed to pay \$3.6 million to American Express to resolve all Data Breach-related issues between the two parties.

**H. Heartland’s “Dream” Payment Card Processing System and Why it Failed.**

**85.** Shortly after the formation of Heartland, Carr, Heartland’s founder and driving force, made the conscious decision to grow the company as rapidly as possible and did what was necessary to do so. Carr was not interested in fitting Heartland into the existing Payment Card processing systems or using time-tested technology. Instead, Carr’s plan was to create a fixed cost Payment Card processing system based on a combination of “off the shelf” hardware, a certain amount of “off the shelf” software and a substantial amount of internally developed software. In other words, Carr determined to create his own Payment Card processing system, which he believed would allow him to undercut his competition. As Baldwin states on the Heartland website, Carr “always had this dream of having his own platform.” [www.heartlandpaymentsystems.com/Technology](http://www.heartlandpaymentsystems.com/Technology).

**86.** Based on information released to date by Heartland and KeyBank about the Data Breach, it appears that Heartland dubbed the “dream” Payment Card processing system platform the “Exchange.” Heartland revealed in its motion to dismiss filed in MDL No. 2046; *In re Heartland Payment Systems, Inc. Customer Data Breach Security Litigation*; in the United States District Court for the Southern District of Texas (Dkt. # 40), that the “Exchange” was the location where the Data Breach occurred. *Id.* at 3.

**87.** According to Heartland, the “Exchange” is a one-of-a-kind “proprietary” platform that first became available for use by Heartland clients in 2001. Heartland developed the Exchange platform internally. *See* Heartland September 30, 2007 Form 10-Q; [www.heartlandpaymentsystems.com/Technology](http://www.heartlandpaymentsystems.com/Technology).

**88.** Soon after the introduction of the “Exchange” in 2001, and apparently as the next step in the development of the “dream” Payment Card processing system, Heartland decided that it wanted direct access to the Visa/MasterCard Networks that, in fact, is normally given only to FDIC regulated financial institutions. A loophole in the regulations governing the Visa/MasterCard Networks, however, allows non-banks like Heartland to directly access the Networks if Heartland became the agent of a “sponsoring bank” that is a “member” of the Visa and MasterCard Associations. Ergo, in April 2002, shortly after rolling out the Exchange platform, Heartland entered into a Merchant Processing Agreement (“MPA”) with KeyBank whereby KeyBank became Heartland’s principal and “sponsor.” At about this time, Heartland also entered into a similar MPA with Heartland Bank.

**89.** The principal benefit to Heartland of the MPAs with the Defendants was direct access to the Visa/MasterCard Networks; access which allowed Heartland to cut Defendants out of the authorization loop and, as a result, reduce costs and bring more fees in-house. Many of the costs eliminated under this model are costs that existed as a result of the security infrastructure at Defendants which, after the MPAs were executed, no longer were part of the authorization loop. Defendants and Heartland recognized this potential exposure and, as a result, the KeyBank/Heartland MPA contains specific provisions requiring Heartland to conduct its business “in accordance with established risk management practices” and protect KeyBank against losses

that might result from Heartland's failures to do so. *See* KeyBank/Heartland MPA at ¶¶ 1.1(e); 1.2(e); 4.5(a). The same is true for the Heartland Bank/Heartland MPA.

**90.** Thus, by early 2002, Heartland's "dream platform," the "Exchange," was in place and ostensibly "ready to go" for the benefit of both Heartland and its sponsors, the Defendants. Development of the Exchange continued for several years and, on information and belief, continues until today.

**91.** During its development, Heartland not only put Confidential Payment Card Data into the Exchange, but rapidly increased the number of Payment Card transactions the system processed, all while acting in the course and scope of its agency relationship with Defendants. According to Heartland's SEC filings and other publicly available materials, its Payment Card processing clients grew dramatically and rapidly in both number and transaction volume processed during the years leading up to the Data Breach:

- 2004: Client number unknown; \$25 billion in transaction volume
- 2005: Client number unknown; \$33.7 billion in transaction volume
- 2006: 133,200 clients generating \$43.3 billion in transaction volume
- 2007: 154,759 clients generating \$51.9 billion in transaction volume
- 2008: 238,000 clients generating \$66.9 billion in transaction volume
- 2009: 250,000 clients generating \$80 billion in transaction volume

*See, e.g.,* Heartland December 31, 2006 Form 10-K; "*Lessons Learned From the Data Breach at Heartland,*" [www.debix.com/webinar/heartland](http://www.debix.com/webinar/heartland) (September 10, 2009) (the "Lessons Learned Webinar").

**92.** During this time, however, not all of Heartland's customers were convinced that the Exchange was properly securing the Confidential Payment Card Data and insisted that their

Payment Card transaction processing be performed by established vendors under contract with Heartland, such as “Vital” (now known as TSYS Acquiring Solutions). According to Baldwin, these customers “insisted” that TSYS Acquiring Solutions (Vital) process their Payment Card transactions because they believed, even as late as 2006, that the Exchange did not have the “proper” security certifications. *ISO & Agent*, Vol. 2, Issue 25 at 3 (May 10, 2006). Defendants recklessly ignored these concerns, ignored their obligations to monitor Heartland’s Payment Card processing system security and allowed Heartland to substantially reduce its Payment Card processing system security costs and maximize its profits.

**93.** The elimination of FDIC regulated banks (*i.e.*, Defendants) from the authorization loop—a security failure that Defendants authorized, permitted and encouraged—in addition to the dramatic increase in Payment Card transaction volume, imposed additional obligations on Defendants to ensure that Heartland’s Payment Card processing system security procedures kept pace with the its growth in the 2002 – 2008 timeframe. This did not happen, however, as evidenced by, among other things, (i) Heartland’s public disclosure that it did not realize it had failed in its efforts to “clean up” the original security breach, and (ii) Heartland’s public concession that all of its security “audits,” performed both prior to and during the Data Breach, were “of no value whatsoever” and “worthless.”

**94.** With respect to the lack of internal security Heartland maintained within the Exchange—a security system that Defendants was obligated to develop, monitor, oversee, supervise and test—it is evident that Heartland’s failures were extensive and Defendants’ failures even worse. According to Carr, as alleged above, the “bad guys” originally accessed the system through a “customer facing web page.” Carr’s direct statements describe generally what happened and how Heartland responded to it:

There was a SQL injection into our system at the end of December, 2007. It was not in our payment system. It was an incident that occurred, actually, in a merchant facing payroll page . . . . We found this SQL injection quickly and we cleaned it up, we thought. Unfortunately, we learned fourteen, thirteen months later that the bad guys had gotten in through this SQL injection and we had not found it. We thought we had cleaned everything up and we had people look to see if we cleaned it up but in fact we had not, they were into our corporate network and eventually were able to cross through and get into our payments network. So, this all began, unbeknownst to us, in December of 2007.

\* \* \*

In very late October of last year (2008) we were informed by a card brand (Visa or MasterCard) that some issuers suspected that we may have been the victim of a breach . . . that card numbers may have been taken from our system. We were given sample transactions . . . we weren't sure exactly what was going on . . . we didn't find a problem.

\* \* \*

From January 13 to January 20 (2009), we did learn about the breach. We had actually been told by one of our forensic companies that, they brought us some data files that looked strange, they were very large 'tmp' files . . . they were not created by any of our systems. And within a few hours of us getting that data our people were able to find malware on our system.

\* \* \*

The remediation that we did was extensive, I think extensive is not a strong enough word, frankly. . . . We reimaged our servers that we knew were involved . . . . We added additional network segmentation into our systems, we created more intense monitoring and developed more intense data loss prevention efforts. One of the things that we did . . . was that we installed Vontu (a software program that finds data being stored on the system that should not have been there) . . . this is a great tool, it's not cheap, but it's a very effective tool in finding card numbers that should not be stored somewhere. We also did every other thing that our forensics companies and the card brands asked us to do in terms of remediation. *At that stage of the game, who were we to say we didn't need one more layer of security?*

See the Lessons Learned Webinar, [www.debix.com/webinar/heartland](http://www.debix.com/webinar/heartland) (emphasis added).

Noticeably absent from Carr's admissions is any reference to any steps taken by Defendants to prevent the intrusion, investigate the intrusion after it was initially identified and/or participate in the planning or implementation of the remedial steps necessary to remedy the situation and

eliminate the security problems going forward. Defendants were simply nowhere to be seen, either before or after any portion of the Data Breach.

**95.** As Carr's statements in his Lessons Learned Webinar reveal, the "intrusion" occurred in 2007, yet neither Heartland's nor Defendants' internal security governing the Exchange *ever* found *anything* amiss until the "tmp" files were identified by a forensics consultant. Carr's admissions also reveal that Defendants' decision making in terms of their oversight responsibilities was extraordinarily poor. Not only did Defendants allow Heartland to operate without having anyone in charge of security at the time of the initial breach in 2007, but they failed to insist that basic software programs like Vontu—which were readily available years before the Data Breach—be utilized by Heartland. Instead, Defendants allowed and condoned Heartland's reliance on annual security "snapshots" of its Payment Card transaction system performed by QSAs *deliberately* selected by Heartland using a "lowest bidder" process—a policy and procedure specifically approved and/or ratified by Defendants.

**96.** According to Carr, the QSAs Defendants approved Heartland to utilize knew nothing about *hundreds* of other similar security lapses at other companies during the time they were auditing Heartland, proving that Defendants permitted Heartland to perform very little due diligence prior to selecting the auditors ([www.csoonline.com/article/print/499527](http://www.csoonline.com/article/print/499527)), and that "you get what you pay for." In fact, the information the QSAs provided to Heartland was, according to Carr, "*of no value whatsoever*." *Id.* (emphasis added). *See also* Lessons Learned Webinar.

**97.** Heartland's use of the cheapest QSA auditors possible (whose annual stamp of "approval" was "worthless" and "of no value whatsoever"), failure to build the appropriate security safeguards in its Payment Card processing system, and failure to hire and install a Chief Security Officer predictably led to disastrous and catastrophic results. In fact, growing Heartland

as quickly as possible without making any real effort to make sure its security measures kept pace with its growth, all without proper oversight by Defendants, relegated the other Visa/MasterCard Association members—such as Plaintiffs and their fellow Issuers—to little more than guinea pig status in the Heartland/KeyBank/Heartland Bank test laboratory.

**98.** Heartland’s use of the Payment Card industry as a laboratory to test the security of its “dream platform” is not a speculative thesis. In fact, prior to the Data Breach, Heartland was fully aware that the manner in which it was building its “dream platform” would lead to problems. *See, e.g.,* Baldwin video interview on the Heartland website ([www.heartlandpaymentsystems.com /Technology](http://www.heartlandpaymentsystems.com/Technology)) (“when it came time for us to build a platform,” it was “*inevitable*” that “missteps” would occur and despite these “inevitable missteps,” the company was “pretty quick to figure them out . . . and keep moving forward.”). And, while “moving forward” was certainly positive for Defendants and Heartland, whose transaction volume in 2009 has, to date, exceeded its 2008 volume by approximately *twenty billion* dollars (\$20,000,000,000), the “inevitable missteps” created disaster for all other parties involved in the processing loop with Heartland and Defendants — such as Plaintiffs and their fellow Issuers damaged by the Data Breach. Heartland played fast and loose with its Payment Card processing system security measures and Defendants, Heartland’s “sponsors” and principals, failed to properly oversee Heartland pursuant to their obligations to Plaintiffs and the other affected Issuer Class members as fellow members of the Associations.

**99.** Serious and extensive losses fell on Issuers—like Plaintiffs and the Issuer class members—who as a predictable result of Heartland’s “inevitable missteps” and Defendants’ complete lack of oversight, were compelled to replace the compromised Payment Cards and sustain billions of dollars in hard financial losses.

**I. The Conduct of Defendants and Heartland after the Data Breach.**

**100.** Upon information and belief, on the day after the Data Breach was publicly announced, Heartland conducted a webinar about the Data Breach for its high level employees, sales representatives and/or relationship managers. Upon information and belief, Heartland's relationship managers were told that PCI-DSS compliance was "not a big deal." Defendants knew or should have known that Heartland's management held PCI-DSS compliance in such low esteem. Defendants were obligated under the FDIC (and related) rules to insist that Heartland comply with all applicable PCI-DSS requirements (at a bare minimum), and verify and validate that Heartland, in fact, was in compliance at all times. Yet Defendants failed to meet these obligations, and the result was predictable—Heartland was not in compliance when it should have been which, in turn, resulted in the Data Breach which, in turn, directly and proximately caused Plaintiffs and all similarly situated financial institutions to incur substantial damages replacing the compromised Payment Cards. As Visa stated after the breach, "no compromised entity has yet been found to be compliance with PCI DSS at the time of a breach."

**101.** For what has been described as potentially the "largest data breach ever"—and which undisputedly includes sensitive financial and banking information—Heartland has publicly taken a cavalier approach regarding the Data Breach. Indeed, in a January 2009 article in *The Washington Post*, Baldwin described the Data Breach as follows:

"The nature of the [breach] is such that card-not-present transactions are actually quite difficult for the bad guys to do because one piece of information we know they did not get was an address," Baldwin said. As a result, he said, the prospect of thieves using the stolen data to rack up massive amounts of fraud at online merchants "is not impossible, but much less likely."

Many states have laws that require entities like Heartland to promptly notify affected consumers when their sensitive personal and/or financial information is compromised in a data breach.

Upon information and belief, Heartland—ostensibly with Defendants’ blessing and ratification—has not sent *any* individualized notice to *any* consumers affected by the Data Breach. Instead, Heartland and Defendants effectively shifted this obligation (and the substantial expense and time associated therewith) to Plaintiffs and other affected Issuers, which have been compelled to issue replacement Payment Cards to their customers and absorb millions of dollars of unauthorized charges, expenses and losses.

**102.** Instead of actively addressing the injuries to Plaintiffs and other affected Issuers that were caused as a result of their negligence and other misconduct, Heartland and Defendants have turned a blind eye to the situation. Indeed, the Question & Answer section on Heartland’s website instructs consumers to notify *the card issuer* of any suspected unauthorized transactions. Defendants have done nothing but blame Heartland.

**103.** It is clear that there are several steps that Defendants should have and could have taken before the Data Breach and steps Heartland should have and could have taken before the Data Breach, any of which would have prevented the Data Breach from occurring in the first place. Significantly, Baldwin reportedly acknowledged as much in an interview conducted immediately after the Data Breach:

There are a host of things we didn't go into that we're implementing, some larger, some smaller, all of which are designed to say, “OK, we had a commitment to high security. We were PCI compliant -- that was certified in April of last year. Yet we had this problem. Clearly we need to do more.” So our IT team is implementing as many additional precautions as it can as quickly as possible.

**104.** On its website, Heartland also states that it is taking numerous precautions going forward that could (and Plaintiffs allege should) have been implemented years ago, precautions that would have been taken prior to the Data Breach had Defendants complied with their oversight responsibilities:

*What are we doing to further secure our systems?*

Heartland immediately took a number of steps to further secure its systems. In addition, Heartland will implement a next-generation program designed to flag network anomalies in real-time and enable law enforcement to expeditiously apprehend cyber criminals. Heartland is deeply committed to maintaining the security of cardholder data, and we will continue doing everything reasonably possible to achieve this objective.

(emphasis added).

**105.** Heartland currently is in the process of implementing an end-to-end encryption process called “E3.” This initiative is designed to encrypt Confidential Payment Card Data from the moment the card is swiped by the merchant until it arrives at its final destination at the Issuer for authorization and settlement. In a January 27, 2009 press release, Heartland stated that it had created an “internal department dedicated exclusively to the development of end-to-end encryption to protect merchant and customer data used in financial transactions.” On an August 4, 2009 Earnings Call with analysts, Carr stated that the E3 end-to-end encryption project will “offer merchants the highest level of beta security in the marketplace.” And, according to a June 17, 2009 press release issued by Heartland, the E3 software “will significantly enhance the security of payment card information throughout the processing lifecycle.”

End-to-end encryption, however, is not a new or novel concept. It could have been instituted years ago by Heartland—on its own or certainly at the insistence of Defendants—but, on information and belief, the concept specifically was rejected by Carr and other Heartland senior management—and ostensibly condoned by Defendants—because of the alleged expense to implement end-to-end encryption and its potential negative impact on Heartland’s earnings. End-to-end encryption also was not required by Defendants, again, because to have required it would have impaired the ability of its agent, Heartland, to process transactions and, therefore, would have directly impacted the profitability of Defendants’ sponsorship of Heartland. As a

direct and/or proximate result of Defendants' wrongful actions and/or inaction, Plaintiffs and other Issuers impacted by the Data Breach (*i.e.*, the Class members) suffered actual financial injuries in the form of, *inter alia*, the costs to cancel and destroy compromised Payment Cards, the costs to issue replacement Payment Cards and the absorption of fraudulent charges made on the compromised Payment Cards. These losses are in the multiple millions of dollars.

### **CLASS ACTION ALLEGATIONS**

**106.** Plaintiffs that are Issuers bring this action as a class action, pursuant to FED. R. CIV. P. 23(a), 23(b)(1), 23(b)(2) and/or 23(b)(3), on behalf of themselves and the following Class of Issuer financial institutions (the "Issuer Class"):

All banks, credit unions, financial institutions and other entities in the United States that issued Visa and/or MasterCard credit cards and/or debit cards and received a Visa and/or MasterCard alert informing them that such credit cards and/or debit cards were compromised by the Heartland Data Breach.

Plaintiffs that are Acquirers bring this action as a class action, pursuant to FED. R. CIV. P. 23(a), 23(b)(1), 23(b)(2) and/or 23(b)(3), on behalf of themselves and the following Class of Acquirer financial institutions (the "Acquirer Class"):

All Acquirer banks, credit unions, financial institutions and other entities in the United States that also issued Visa and/or MasterCard credit cards and/or debit cards and received a Visa and/or MasterCard alert informing them that such credit cards and/or debit cards were compromised by the Heartland Data Breach.

Plaintiffs that are Subrogees of financial institution Class members bring this action as a class action, pursuant to FED. R. CIV. P. 23(a), 23(b)(1), 23(b)(2) and/or 23(b)(3), on behalf of themselves and the following Class of Subrogees (the "Subrogee Class"):

All insurance companies, bond issuers and other entities that have paid money to financial institutions pursuant to contractual obligations to indemnify the financial institutions for their losses resulting from the Heartland Data Breach that have asserted and/or could assert subrogation claims as a result.

**107.** Excluded from the proposed Classes are Defendants, Heartland and their parent corporations, subsidiary corporations, brother-sister corporations, affiliates, agents and representatives.

**108.** Upon information and belief, the proposed Issuer Class, Acquirer Class, and Subrogee Class each consist of hundreds—if not thousands—of geographically dispersed members, the joinder of which in one action is impracticable. Disposition of the claims in a class action will provide substantial benefits to both the Parties and the Court.

**109.** The rights of each member of the proposed Classes were violated in a similar fashion based on Defendants' uniform wrongful actions and/or inaction in sponsoring, monitoring and supervising their agent, Heartland, which acts and omissions directly and/or proximately resulted in the Data Breach and the injuries suffered by Plaintiffs and the members of the proposed Classes.

**110.** The following questions of law and fact are common to the proposed Classes, and predominate over questions that may affect individual Class members:

- (i) Whether Defendants failed to monitor, audit and confirm that Heartland's Payment Card processing system safeguards were in place and fully operational in order to protect the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and proposed Acquirer Class (*i.e.*, the customers for whom Plaintiffs and the members of the proposed Issuer Class and proposed Acquirer Class replaced their Payment Cards compromised by the Data Breach and/or absorbed the related unauthorized charges)?
- (ii) Whether Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class are intended third party beneficiaries of the MPAs between Defendants and Heartland and, if so, whether Defendants breached the MPAs vis-à-vis Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class?
- (iii) Whether Defendants owed fiduciary duties to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class as Visa and/or MasterCard Association joint venture members and, if so, whether Defendants breached such fiduciary duties?

- (iv) Whether Defendants were negligent in monitoring, auditing and confirming whether Heartland's Payment Card processing system safeguards were in place and fully operational in order to protect the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class (*i.e.*, the customers for whom Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class replaced their Payment Cards compromised by the Data Breach and/or absorbed the related unauthorized charges)?
- (v) Whether Defendants are vicariously liable for the wrongful actions by and/or inaction of Heartland, Defendants' agent?
- (vi) Whether Defendants' actions and/or inaction proximately caused damages to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class?
- (vii) Whether Plaintiffs and the members of the Classes are entitled to compensation, monetary damages and/or any other services/corrective measure(s) from Defendants and, if so, the nature and amount of any such relief?

**111.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the proposed Classes they are designated to represent. Plaintiffs do not have any interests antagonistic to and/or in conflict with the interests of the other members of the respective Classes.

**112.** Plaintiffs are represented by counsel competent and experienced in the prosecution of data breach litigation, complex commercial litigation and class actions.

**113.** Defendants have acted or refused to act on grounds generally applicable to the members of the proposed Classes, thereby making appropriate equitable relief with respect to them.

**114.** Members of the proposed Classes are readily ascertainable. By definition, the members of the Issuer and Acquirer Classes were notified that certain Payment Cards issued by them were compromised by the Data Breach, and thereafter replaced all or a portion of such

compromised Payment Cards at substantial expense. The members of the Subrogee Class made payments to members of the proposed Issuer Class and proposed Acquirer Class.

**115.** Prosecuting separate actions by individual members of the proposed Classes would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendants. Moreover, adjudications with respect to individual members of the proposed Classes, as a practical matter, would be dispositive of the interests of the other members of the respective Classes.

**116.** Certification of the proposed Classes, therefore, is appropriate pursuant to Rule 23(b)(1), (b)(2) and/or (b)(3) of the Federal Rules of Civil Procedure.

## **CLAIMS AND CAUSES OF ACTION**

### **COUNT I**

#### **BREACH OF CONTRACTS TO WHICH PLAINTIFFS AND THE MEMBERS OF THE PROPOSED ISSUER CLASS AND THE PROPOSED ACQUIRER CLASS ARE INTENDED THIRD PARTY BENEFICIARIES**

##### **(ON BEHALF OF THE PROPOSED ISSUER AND ACQUIRER CLASSES)**

**117.** The preceding factual statements and allegations are incorporated herein by reference.

**118.** Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class are intended third-party beneficiaries of contracts entered into between Defendants and various entities. These contracts include, without limitation, the MPAs between Defendants and Heartland (*see, e.g.*, the KeyBank/Heartland MPA at ¶¶ 1.1(e); 1.2(e); 4.3(b); 4.5(a)) as evidenced by, *inter alia*, the lack of any provision in the MPA expressly or impliedly disclaiming the intent of KeyBank and Heartland to create third party beneficiaries—even after KeyBank and Heartland amended the MPA in 2006 with full knowledge of the developing body

of third party beneficiary case law in the Payment Card processing arena. The same is true with respect to the Heartland Bank/Heartland MPA.

**119.** Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class are intended third-party beneficiaries of contracts entered into between Defendants and various entities. These contracts include, without limitation, the MPAs between Defendants and Heartland as evidenced by the circumstances, the duty by Defendants and Heartland to secure the Confidential Payment Card Data of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, and the actions of Defendants and Heartland that are consistent with the MPAs, which expressly and/or impliedly require that, *inter alia*, (i) Heartland take the appropriate steps necessary to safeguard the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, and (ii) Defendants monitor, audit, oversee and confirm that Heartland's Payment Card processing system safeguards were adequate and complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained and were fully operational in order to protect the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class.

**120.** Under the circumstances, recognition of a right to performance of the MPAs by Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class is appropriate to effectuate the intentions of Defendants and Heartland. The Defendants and Heartland intended to give Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class the benefit of the performance promised in the MPAs.

**121.** Heartland breached the MPAs by, *inter alia*, failing to adequately safeguard the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class (as set forth in detail above). Defendants breached the MPAs by, *inter alia*, failing to monitor, audit, oversee and confirm that Heartland's Payment Card processing system safeguards were adequate and complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained and were fully operational in order to protect the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class.

**122.** The breach of the MPAs by Defendants and Heartland (as set forth in detail above) directly and/or proximately caused Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class to suffer substantial damages in the form of, *inter alia*, the costs to cancel and destroy compromised Payment Cards, the costs to issue replacement Payment Cards to their customers affected by the Data Breach and the absorption of fraudulent charges made on the compromised Payment Cards.

## **COUNT II**

### **BREACH OF FIDUCIARY DUTY**

#### **(ON BEHALF OF THE PROPOSED ISSUER AND ACQUIRER CLASSES)**

**123.** The preceding factual statements and allegations are incorporated herein by reference.

**124.** By virtue of their membership in the Visa and MasterCard Associations, the operating rules and regulations of such Associations and the applicable law and regulations, Defendants, on the one hand, and Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, on the other hand, were (and continue to be) in confidential, special

and fiduciary relationships with each other, such relationships creating and/or emanate out of a joint venture.

**125.** As their fiduciaries and co-joint venturers, Defendants owed Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class (i) the commitment to deal fairly and honestly, (ii) the duties of good faith and undivided loyalty, and (iii) integrity of the strictest kind. Defendants were (and continues to be) obligated to exercise the highest degree of care in carrying out their obligations to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class under their confidential, special and fiduciary relationships.

**126.** Defendants breached their fiduciary duties to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class by, *inter alia*, failing to monitor, audit, oversee and confirm that Heartland's Payment Card processing system safeguards were adequate and complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained and were fully operational, all in order to protect the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class (as set forth in detail above).

**127.** To the extent Defendants are not fiduciaries or co-joint venturers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, Defendants nevertheless incurred fiduciary liability to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class because they had knowledge of the breaches of fiduciary duties committed by Heartland, another fiduciary of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, including, *inter alia*, failing to safeguard the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed

Issuer Class and the proposed Acquirer Class (as set forth in detail above), and did not make reasonable efforts under the circumstances to remedy such fiduciary breaches.

**128.** To the extent that Defendants are not fiduciaries or co-joint venturers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, Defendants nevertheless incurred fiduciary liability to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class in that Defendants engaged in transactions with Heartland, another breaching fiduciary of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, under circumstances in which Defendants knew (or should have known) about such fiduciary breaches including, *inter alia*, Heartland's failure to safeguard the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class (as set forth in detail above), and did not make reasonable efforts under the circumstances to remedy such fiduciary breaches..

**129.** Defendants breached their fiduciary duties to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class through the wrongful actions and/or inaction set forth in detail above. Defendants willfully and wantonly breached their fiduciary duties to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class or, at the very least, committed these breaches with conscious indifference and reckless disregard of their rights and interests. Defendants' wrongful actions constitute breach of fiduciary duty.

### **COUNT III**

#### **NEGLIGENCE**

#### **(ON BEHALF OF THE PROPOSED ISSUER AND ACQUIRER CLASSES)**

**130.** The preceding factual statements and allegations are incorporated herein by reference.

**131.** By virtue of, *inter alia*, (i) the special relationships between Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, on the one hand, and Defendants, on the other hand, (ii) the finite, well-defined and limited class of members of the Associations (who are the Plaintiffs and members of the two Classes alleged herein), all of whom were known to exist by Defendants, (iii) the foreseeable manner by which data losses resulting from the acts and/or omissions of one Association member affect and impact the other members of the Associations, (iv) the foreseeability of the damages incurred by Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class as a result of a data breach within the Associations—such as the Heartland Data Breach, and (v) the vast array of responsibilities and obligations imposed on Defendants and their agent, Heartland, through the FDIC and FFIEC recommendations and guidelines, Defendants had (and continue to have) a duty to exercise reasonable care in monitoring, auditing, overseeing and confirming that Heartland’s Payment Card processing system safeguards were adequate and complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained and were fully operational, all in order to protect the Confidential Payment Card Data of the customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class. Specifically, Defendants, *inter alia*:

- wrongfully and negligently allowed Heartland to be PCI-DSS non-compliant at the time of the Data Breach because Defendants had no ongoing validation process designed to maintain, at the bare minimum, PCI-DSS compliance at Heartland—even though Defendants knew Heartland was processing tens of millions of transactions monthly. Defendants knew and/or should have known (due to prior well-publicized data breaches, such as the TJX and Hannaford Brothers data breaches, which Defendants knew about) that huge numbers of transactions with extremely sensitive data create a huge security risk which, in turn, requires enhanced oversight and constant monitoring and auditing to confirm that Heartland’s Payment Card processing system safeguards were in place and fully operational in order to protect the Confidential Payment Card Data of the

customers of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class.

- knew and/or should have known (due to prior well-publicized data breaches, such as the TJX and Hannaford Brothers data breaches, which Defendants knew about) that a high risk area for a data breach is between the merchants and Heartland. Defendants failed to establish an appropriate risk management process that identified, measured and limited such risks. Rather, Defendants abdicated their oversight obligations by relying on QSA audits that were clearly deficient (as Carr admitted) and/or with knowledge that Heartland was selecting the lowest bidders for its QSAs.
- should have implemented their own internal audit coverage that should have included assessments of the design and implementation of Heartland's security measures, including Heartland's own internal IT audit, internal control, management policies and procedures at all Heartland data centers or sites where intrusion was possible.
- should have implemented a system of operational risk controls that included information system, procedural, administrative and legal measures to prevent financial losses as a result of operational risk—including encryption to ensure transaction information integrity.
- failed to evaluate the effectiveness of the Heartland Payment Card processing system configuration, firewalls, intrusion detection protocols and other similar controls, if any, that Heartland had in place and/or should have had in place that would have prevented the Data Breach.
- failed to evaluate the effectiveness of the Heartland Payment Card processing system configuration, firewalls, intrusion detection protocols and other similar controls, if any, that Heartland had in place and/or should have had in place that would have prevented the Data Breach.
- failed to put into place a comprehensive security vendor management and review program.
- failed to utilize external audits, physical visits to ensure security and/or adequate operational controls vis-à-vis its obligation to oversee Heartland, their agent.
- failed to implement an ongoing security process and institute appropriate governance for the security function in at least five primary areas, including Information Security Risk Assessment, Information Security Strategy, Security Controls Implementation, Security Monitoring and Security Process Monitoring and Updating.
- failed to adopt measures that limit operational risks for the processing, clearing and settlement of retail payments by Heartland; this risk analysis should have

identified confidential assets, critical operations, and potential threats and defined safeguards and countermeasures to provide adequate protection.

- failed to protect against the risk of malicious code by implementing appropriate controls at the host and network level of Heartland's Payment Card processing system to prevent and detect malicious code, including the use of controls that utilize technology, policies and procedures and training, all applied in a layered manner from perimeters inward to hosts and data.
- failed to secure access to Heartland's computer networks through multiple layers of access controls to protect against unauthorized access.
- failed to employ encryption to mitigate the risk of disclosure of sensitive information in transit.
- failed to maintain an ongoing information security risk assessment program that effectively gathers data regarding the information and technology assets of Heartland, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements.
- failed to require controls that would have required Heartland, when deploying off the shelf software, to harden the resulting system.
- failed to independently review Heartland's security through appropriate audits and tests, to ensure that Heartland implemented adequate security controls to safeguard Confidential Payment Card Data, relying instead on Heartland's SAS 70 (*i.e.*, QSA) audits—which was especially negligent given the high risk nature of Heartland's business model and proprietary "Exchange" platform.
- failed to carefully and critically evaluate whether a SAS 70 report adequately supported Defendants' oversight responsibilities, failed to recognize that the SAS 70 reports obtained by Heartland under the "lowest bidder" process did not address the effectiveness of the security process in continually mitigating changing risks, and failed to address whether Heartland met Defendants' specific risk mitigation requirements.
- failed to use the guidance in the FFIEC and FDIC manuals, handbooks and booklets in exercising its ongoing oversight and audit responsibilities.

- failed to continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on other Payment Card system users, and the effectiveness of existing security controls, and further failed to use such information to update the risk assessment, strategy, and implemented controls at Heartland, instead, relying on a static security system program that created a false sense of security and became increasingly ineffective over time.

**132.** Defendants, by and through their above negligent actions, inaction and/or omissions, unlawfully breached their duties to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class.

**133.** But for Defendants' negligent and wrongful breaches of the duties they owed (and continue to owe) to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, their customers' Confidential Payment Card Data would never have been wrongfully disseminated, the Data Breach would not have occurred and Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class would not have incurred multiple millions of dollars notifying their customers about the Data Breach, canceling, destroying and replacing Payment Cards compromised by the Data Breach and/or absorbing unauthorized charges made on the compromised Payment Cards.

**134.** The Data Breach and the above-described substantial injuries suffered by Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class were (and continue to be) a direct and/or proximate result of Defendants' abdication of their responsibility to monitor, audit, oversee and confirm that Heartland's Payment Card processing system safeguards were adequate and complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained and were fully operational. The Data Breach and the above-described substantial injuries suffered by Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class also were a reasonably foreseeable consequence of Defendants' negligence and/or gross negligence.

To the extent Defendants assert that the economic loss doctrine bars the claims of Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class, Plaintiffs affirmatively state that the economic loss doctrine does not apply because (i) Issuer financial institutions—such as Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class—were not in express contractual privity with Defendants and/or Heartland and could not protect their economic interests via express contracts, and (ii) the basis of their indirect relationships is not a tangible product, but rather an intangible service.

#### **COUNT IV**

#### **VICARIOUS LIABILITY**

#### **(ON BEHALF OF THE PROPOSED ISSUER AND ACQUIRER CLASSES)**

**135.** The preceding factual statements and allegations are incorporated herein by reference.

**136.** Once Defendants and Heartland entered into their respective MPAs, Defendants allowed Heartland to utilize their BINs (Bank Identification Number), although Defendants retained full and unfettered control over the BINs and how, when and under what circumstances the BINs could be used by Heartland. As stated by Heartland in its SEC filings, the KeyBank BIN allowed Heartland “to route Visa and MasterCard transactions *under the member bank’s [i.e., KeyBank’s] control . . . to clear credit bank card transactions through Visa and MasterCard.*” (emphasis added).

**137.** Once Defendants and Heartland entered into their respective MPAs, Defendants had the right (and concomitant obligation) to compel Heartland to provide them with any and all information pertaining to Heartland’s compliance with the Visa and MasterCard rules and regulations and any other information pertaining to the methods and systems used by Heartland to protect Confidential Payment Card Data.

**138.** Once Defendants and Heartland entered into their respective MPAs, Defendants had full authority (and the concomitant obligation) to inspect, monitor, test, examine, audit, oversee, and confirm that Heartland's Payment Card processing system safeguards were adequate and complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained and were fully operational. In this regard, Defendants had the right (and concomitant obligation) to control Heartland's Payment Card system security protocols and programs.

**139.** Once Defendants and Heartland entered into their respective MPAs, Heartland was permitted to acquire merchants on behalf of Defendants, but Defendants had the right (and concomitant obligation) to control and, in fact, controlled the ultimate decision whether to accept a particular merchant as a customer.

**140.** Once Defendants and Heartland entered into their respective MPAs, Heartland became Defendants' "agent" as that term is defined under the operating rules and regulations of both Visa and MasterCard.

**141.** At all relevant times, including the time of the Data Breach and during the loss of the Confidential Payment Card Data, Heartland utilized BINs owned and controlled by defendants "to route Visa and MasterCard transactions *under the member bank's control* . . . through Visa and MasterCard." (emphasis added). The loss of the Confidential Payment Card Data occurred during the process of "routing" the data, *i.e.*, while "under the member bank's control."

**142.** At all relevant times, Defendants were the principals of Heartland, Heartland was the agent of Defendants and Heartland acted in the course and scope of its agency and authority conferred on it by Defendants.

**143.** At all relevant times, Defendants expressly and impliedly gave Heartland the authority to act on their behalf within the Associations and retained the right to control and direct the details, manner and/or means by which Heartland could conduct its business activities in the Associations, including the details, manner and/or means by which Heartland should have secured the Confidential Payment Card Data as it was being routed through the Networks.

**144.** Heartland's wrongful actions, inaction and/or omissions that resulted in the Data Breach were part of its Payment Card processing business operations, which were conducted pursuant to its agency relationship with Defendants. Nothing Heartland did at any time constituted a departure from the scope of its authority to utilize the services provided by the Associations.

**145.** Nothing Heartland did or failed to do was forbidden by Defendants.

**146.** Nothing Heartland did was contrary to the authority given to it by Defendants.

**147.** Nothing Heartland did constituted a departure from the business in which Defendants authorized it to engage. Rather, Defendants fostered, ratified and authorized the manner in which Heartland developed, monitored, tested and audited the security measures it used in an to attempt to secure the Confidential Payment Card Data it processed and "routed" through the Networks.

**148.** Nothing Heartland did in terms of "routing" Confidential Payment Card Data through the Networks was for the sole benefit of Heartland. Rather, "routing" Confidential Payment Card Data through the Networks provided substantial revenue and profits for Defendants.

**149.** Everything Heartland did and did not do pertaining to the alleged security of its Payment Card processing system and the Data Breach itself—before, during and after the Data Breach—was ratified and approved by Defendants, Heartland’s principals.

**150.** As a member of the Associations and *by and through their conduct as described above*, Defendants caused the other members of the Associations (*i.e.*, Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class) to believe that Defendants would fully comply with its obligations to monitor, audit, oversee and confirm that Heartland’s Payment Card processing system safeguards were adequate and complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained, and were fully operational.

**151.** Defendants knew that Plaintiffs—as co-joint venturers in the Associations—believed that they would fully comply with their obligations to monitor, audit, oversee and confirm that Heartland’s Payment Card processing system safeguards were adequate and complied with all applicable laws and guidance, were in place, were being properly monitored, managed, updated and maintained and were fully operational. Despite this knowledge, Defendants failed to advise Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class that they were not living up to their obligations, but instead, gave Heartland free reign to attempt to secure the Confidential Payment Card Data while it was processed by Heartland and “routed” through the Networks.

**152.** Defendants are responsible for the wrongful actions, inaction, omissions and/or negligence of their agent, Heartland, which, in whole or in part, directly and/or proximately caused and/or allowed the Data Breach to occur and Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class to incur the substantial damages they have incurred

(and continue to incur). Defendants are responsible to Plaintiffs and the members of the proposed Issuer Class and the proposed Acquirer Class for all such damages.

## COUNT V

### **CLAIMS OF THE SUBROGEE CLASS MEMBERS**

**153.** The preceding factual statements and allegations are incorporated herein by reference.

**154.** The Subrogee Class members stand in the shoes of the members of the proposed Issuer Class and the members of the proposed Acquirer Class to whom they have made payments in satisfaction of their contractual obligations to reimburse for losses caused by the Heartland Data Breach. Accordingly, to the extent the Subrogee Class members are subrogated to claims of the members of the proposed Issuer Class and the members of the proposed Acquirer Class, they hereby assert all such claims.

### **RELIEF REQUESTED**

**155.** The preceding factual statements and allegations are incorporated herein by reference.

**156. ACTUAL DAMAGES.** As a direct and/or proximate result of Defendants' wrongful actions, inaction and/or omissions (as set forth in detail above), Plaintiffs and the members of the proposed Classes have sustained damages (and continue to sustain damages) in the form of, *inter alia*, the (i) costs to cancel and destroy compromised Payment Cards and close associated accounts, (ii) costs to issue replacement Payment Cards and open new accounts and (iii) absorption of fraudulent charges made on the compromised Payment Cards. All of the damages sustained by Plaintiffs and the members of the proposed Classes were reasonably foreseeable by Defendants, and exceed the minimum jurisdictional limits of this Court. All conditions precedent to

the claims of Plaintiffs and the members of the proposed Classes for relief have been performed and/or have occurred.

**157. INJUNCTIVE RELIEF.** Plaintiffs and the members of the proposed Classes are also entitled to injunctive relief, *inter alia*, requiring Defendants to comply with their obligations to monitor, audit, oversee and confirm that Heartland's Payment Card processing system safeguards are adequate and comply with all applicable laws and guidance, are in place, are being properly monitored, managed, updated and maintained and are fully operational in order to secure the Confidential Payment Card Data on a going forward basis, minimize the damage from the Heartland Data Breach and/or minimize the likelihood of future data breaches. Injunctive relief is required because money damages alone are insufficient to redress the irreparable harm Plaintiffs and the members of the proposed Classes face absent these injunctive measures. All conditions precedent to the claims of Plaintiffs and the members of the proposed Classes have been performed and/or have occurred.

**158. ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiffs and the members of the proposed Classes also are entitled to recover their reasonable and necessary attorneys' fees, litigation expenses and court costs in prosecuting this action.

\* \* \*

**WHEREFORE**, Plaintiffs, individually and on behalf of the members of the proposed Issuer Class, the proposed Acquirer Class and the proposed Subrogee Class respectfully request that (i) Defendants be required to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class Representatives, and (iv) Plaintiffs' Counsel be appointed as Class Counsel. Plaintiffs, individually and on behalf of the members of the proposed

Issuer Class, the proposed Acquirer Class and the proposed Subrogee Class further request that upon final trial or hearing, judgment be awarded against Defendants, jointly and severally, for:

- (i) actual damages to be determined by the trier of fact;
- (ii) pre- and post-judgment interest at the highest legal rates applicable;
- (iii) appropriate injunctive and/or declaratory relief;
- (iv) reasonable attorneys' fees and litigation expenses incurred through the trial and any appeals of this case;
- (v) costs of suit; and
- (vi) such other and further relief that this Court deems just and proper.

**JURY DEMAND**

Plaintiffs respectfully demand a trial by jury on all claims and causes of action so triable.

Dated: January 19, 2010

Respectfully submitted,

By:



Michael A. Caddell  
Cynthia B. Chapman  
Cory S. Fein  
CADDELL & CHAPMAN  
1331 Lamar, #1070  
Houston TX 77010  
713.751.0400 (phone)  
713.751.0906 (fax)  
[MAC@caddellchapman.com](mailto:MAC@caddellchapman.com)

Richard L. Coffman  
THE COFFMAN LAW FIRM  
First City Building  
505 Orleans St., Ste. 505  
Beaumont, TX 77701  
(409) 833-7700  
(866) 835-8250  
[rc@cofflaw.com](http://rc@cofflaw.com)

Joseph G. Sauder  
Matthew D. Schelkopf  
Benjamin F. Johns  
CHIMICLES & TIKELLIS LLP  
One Haverford Centre  
361 West Lancaster Avenue  
Haverford, PA 19041  
Telephone: (610) 642-8500  
Facsimile: (610) 649-3633  
[JGS@chimicles.com](mailto:JGS@chimicles.com)

***Proposed Interim Co-Lead Counsel for the Plaintiffs***

Natalie Finkelman  
Shepherd Finkelman Miller & Shah, LLP  
35 E State Street  
Media , PA 19063

R Douglas Gentile  
Douthit Frets Rouse Gentile & Rhodes LLC  
903 East 104th St, Ste 610  
Kansas City , MO 64131

Christopher G Hayes  
Law Office of Christopher G. Hayes  
225 South Church St  
West Chester, PA 19382

Jeffrey L Kodroff  
Spector Roseman Kodroff & Willis, P.C.  
1818 Market St, Ste 2500  
Philadelphia , PA 19103

Mitchell A Toups  
Weller, Green, Toups & Terrell, LLP  
PO Box 350  
Beaumont , TX 77704

Gregory Weiss  
Leopold~Kubin, P.A.  
2925 PGA Blvd  
Palm Beach Gardens , FL 33410

John R. Wylie  
Futterman Howard Watkins Wylie & Ashley, Chtd.  
122 S. Michigan Ave., Suite 1850  
Chicago, IL 60603  
(312) 427-3600  
Fax: (312) 427-1850

***Proposed Steering Committee Counsel for the  
Plaintiffs***